Issues in Incorporating Probabilistic Safety Assessment (PSA) in the Design and Licensing Stages of Generation IV Reactors

Ibrahim A. Alrammah

ibrahim.alrammah@postgrad.manchester.ac.uk

School of Mechanical, Aerospace and Civil Engineering (MACE), University of Manchester, Manchester, United Kingdom

ABSTRACT

Probabilistic approaches has been used and are also highly recommended to be used from the very early stage of the reactor design process. So far, Probabilistic Safety Assessment (PSA) approach is increasingly being utilized in the demonstration of safety in combination with deterministic approaches (e.g. to justify the classification of situations, to determine the sequences of sophisticated failures) and used also to verify the systems and components reliability in order to satisfy safety targets. However, epistemic problems such as uncertainties due to lack of design information, unknown phenomena, plant-specific hazards, data, etc., are larger than that from existing reactors, and will impose a significant challenge to the decision makers. This paper will discuss some technical issues related to applying PSA in the design and licensing stages of Generation IV reactors. These aspects include: initiating events, passive systems modeling, reliability data, common cause failure (CCF), modeling of novel design features, modeling of preventive maintenance, technical specifications, human reliability analysis (HRA), systems interdependencies, modeling of instrumentation and control (I&C), external hazards, continuous design risk monitoring, supporting studies, interpretation of PSA results for new plants.

Keywords: PSA, Generation IV Reactors, CCF, HRA

1. INTRODUCTION

It has been widely accepted that nuclear power has a vital role to play in satisfying the increasing global energy needs. Most operating commercial NPPs around the world are of Generation-II category. The Gen-III reactors have just started operating, and Gen-III+ reactors are at the advanced phase of commercialization. The first reactors of the Generation IV concepts are foreseen to start operating in the period 2020-2030. However, nuclear safety has become an important issue of public concern, especially after the event of Fukushima in March 2011. In order to improve public perception, engineers and designers will have to show a satisfactory level of nuclear safety. Because of this, the Generation IV concepts will likely launch considerable innovative technological changes in comparison with current designs and these innovations will have to be at a higher level of safety.

Although the safety and reliability of these types of reactors are meeting high standards, Generation-IV reactor systems are targeting toward a joint target of providing safer, more reliable, proliferation-resistant and economically feasible nuclear power source. Six design systems have been nominated over others for particular research, development and deployment. They are: Gas-cooled Fast Reactor (GFR), Lead-cooled Fast Reactor (LFR), Molten Salt reactor (MSR), Sodium-cooled Fast Reactor (SFR), Very High Temperature Reactor (VHTR), Super Critical Water-cooled Reactor (SCWR). More safety enhancement for Generation IV concepts can be achieved through evolution in knowledge, technologies and the development of a solid safety methodologies in the early design stages. Such enhancements will particularly address the pathway to attain the safety level by the employment of safety concepts that would be "built-in" to the proposed design concept instead of "added on" to an existing system. The design process Generation IV concepts should be guided by a "risk-informed" methodology (i.e. utilizing both deterministic and probabilistic techniques). Safety of Generation IV concepts can be enhanced by properly implementing, as a supplement of the

deterministic techniques, the probabilistic approaches such as PSA and other techniques as guiders of the design process. [1, 2]

One of the most effective and mature safety tools is the Probabilistic Safety Assessment (PSA). It is considered as an essential approach to achieve enhanced safety for Generation-IV reactor systems. In the past, the design of NPPs was mainly based on deterministic methods. PSA has been recently used to support deterministic criteria and analyses in the design process for new reactor concepts in several projects. In the framework of design, construction and licensing of innovative reactors, PSA plays a vital role as a supplement to traditional deterministic approaches. The importance of applying PSA in the development of new reactor designs is well recognized.

PSA has become a very complex method to identify scenarios of possible accident, quantitatively estimate their occurrence probabilities in a certain time period, and probabilistically estimate the consequences following postulated accidents based on a set of consequence parameters. Along with the conventional deterministic techniques, the approach has come to be broadly accepted as one of the foundations for confirming the safety of a NPP (as well as other installations) worldwide. Until recently, PSA technique was mainly utilized after the design was settled, or even after the plant was constructed. Applied in this stage, PSA was basically used as a tool of estimating the risk level associated with an operating plant. With the development of future evolutionary designs (such as Generation IV concepts), however, the significance of PSA as a vital driver for the design process is perceived. Concurrently, limitations and challenges have to be considered, mainly when the PSA tool is performed for innovative concepts characterized by great uncertainties; lack of precise knowledge and lack of empirical data about failure, provisions and degradation. [1,2]

The main advantages of applying a PSA during the design stage are related to the identifying of plant vulnerabilities, of inter-systems dependencies and potential Common Cause Failures (CCFs), and to the examination of risk levels from different design alternatives. The probabilistic insights will help with the design optimization of safety systems (particularly in terms of diversification and redundancy), and with the checking of the design homogeneity from safety standpoint and, in the near future, from cost to safety benefit concern. [3] Several published studies applies PSA to a reactor concept in the design stage, such as in: [4-12]

The application of PSA to novel systems faces some challenges. Applying a PSA for a plant in the design stage is quite different than applying it for an existing or operating plant in which most of PSA guidance and procedures are formulated. The key challenge in the application of PSA methodology to enhance the plant safety in the pre-conceptual design stage is the lack of information, which increases the uncertainties accompanying any quantitative risk measure. The absence of plant-specific operations procedures and operating experience data at the design stage lead to PSA results that do not reflect the future as-built, as-operated plant. A vague understanding of probable accident scenarios may become an obstacle to the building of risk-informed regulatory initiatives. The methodological challenges include the necessity to address a wide spectrum of systems and phenomena, the potential lack of key reliability and experimental data, the potential lack of knowledge on new main phenomena and the potential lack of accident analysis models. These challenges can influence a variety of factors (e.g. risk balanced concept, defense in depth assessment and plant safety level assessment, etc.) The technical challenges of the PSA for more advanced reactors, which are in research phase or in the early stages of conceptual design, as well as the aforementioned aspects, also comprise the potential requirement to consider very diverse systems and phenomenology. [13]

Currently operating NPPs had a deterministically-launched licensing basis before plant-specific or generic safety information and insights were made obtainable through PSAs. The PSAs generally proved that the original deterministic methodology to licensing was conservative (e.g., plants might respond to some failure scenarios in behaviors that were not attributed in the deterministic analyses) and additionally identified alterations that could enhance plant design and safety. Satisfying the deterministic requirements meant that application of their associated provisions embodied within the models of defense-in-depth, quality assurance, safety margins, conservative assumptions and analyses, and several other factors (numerous of which are not easily measurable

within a PSA model) created a safety basis where the uncertainties were acceptable. However, PSA models have to depend on realistic data to ensure that the main risk insights are not hidden by falsely biased results resulting from the application of irregular conservatisms. Consequently, considerable care must be exercised in performing PSAs in the pre-conceptual design stage to ensure that the essential pillars of deterministic safety process are not unjustifiably compromised. Therefore, for future reactors, use of risk data can have a far more important impact on the safety foundation of the plant, including the ability to derive some main design decisions. [14] In the following sections, some technical issues in applying PSA to novel reactor designs will be discussed.

2. ISSUES IN INCORPORATING PSA IN THE DESIGN AND LICENSING STAGES OF GENERATION IV REACTORS

The main challenge in the utilization of PSA techniques to support the design of a NPP is the lack of information, which exponentially increases the uncertainties associated to any quantitative risk measure that can be associated to an early design. With the evolution of the design, as more information comes to be available, risk metrics become more realistic but they still need to be closely watched for the associated model uncertainties. The assumption/uncertainty database is going to track design alternatives in the form of different event trees or different fault trees explicitly modeled in the PSA, which will identify the uncertainty bounds for the damage and release frequency values. [15]

Another challenge to the use of PSA in design phase is the lack of a recognized standard against with to compare the technical adequacy of a PSA developed for a non-operating reactor, this in the view of the fact that the current PSA standard is dedicated to operating reactor and has requirements that are clearly not applicable until operation of the plant has commenced. [16,17] The following sections discuss issues related to applying PSA in the design and licensing stages of generation IV reactors.

2.1. Initiating Events

For Generation IV reactors, the initiating events list is typically established based on comparable existing reactors PSA and based on generic references like IAEA and NUREG handbooks. This list is then combined with some specific analysis to consider the unique characteristics of the new designs. The resulting initiating events list usually includes some new initiating events specific to the unique plant design features. [18] However, this method does not ensure completeness of the list, particularly if the definition of initial boundary conditions is not complete or not required for the goals of the design PSA (e.g., the loss of I&C initiators or loss of ventilation initiators might be excluded). [19]

2.2. Passive Systems Modeling

Several new NPP designs utilize passive safety systems. Owing to the specificities of passive systems that apply natural circulation (lack of data, small driving force, large uncertainties, etc.), there is a necessity for developing consistent approaches and methodologies for assessing their reliability. With the purpose of increasing confidence in the attained results, it is required to decrease the level of uncertainty associated with the passive system behavior, especially the phenomenological uncertainty. It is also required to determine the dependencies among the related parameters adopted to examine the system reliability. Another important issue is to study the dynamic aspects of the system performance. However, in many of the existing design PSAs, the passive systems models take into account only the failure of the systems components (e.g., pipe break, spurious valves actuation, etc.), and ignore the failure of the phenomena (such as natural circulation).

This issue may need to be addressed by modeling, for example, the scenario dependent situations which may result in a combination of conditions in which the passive system function cannot be executed. The modeling of passive systems in the PSA needs also to consider the impact on other PSA issues. For example, the functioning of the passive systems for extended term accident

scenarios ought to be carefully studied. Another important matter is the treatment of the uncertainties of physical and thermal hydraulic data as well as of the uncertainties in the passive systems behavior.

For PSA supporting studies, the current thermal hydraulic codes might not be entirely applicable for the passive systems behavior analysis. Indeed, the main two issues with thermal hydraulic codes are:

1) When the input parameters are varied over their potential ranges, are the codes still within their domain of applicability or not?

2) Does the analysis consider the possibility of degraded conditions (e.g., subsequent to a seismic event) or not?

2.3. Reliability Data

The assumption that the evolutionary components have the same reliability as the existing ones might be a reasonable initial assumption. Therefore, reliability data and CCF parameters for the components included in the PSA for new reactors are extracted from the same sources as for the PSA for existing reactors. [18]

The method to select the most appropriate data sets depends on the assessment of similarity of the novel reactor components with the existing obtainable data. This approach is adequate in principle. Nevertheless, the similarity investigation between novel reactor components and the existing reactor which was used to calculate the existing reliability data is not a simple task. This evaluation has to take into account, besides the component category and safety level, also the operating conditions, the component population used to calculate the data, the surveillance requirements (test intervals), the recent operating experience trends, the operating environment and parameters (temperature, pressure, flow rates, ambient temperature and humidity), etc. The justification of selecting a given data has to be completely traceable and documented. [19]

Some analysts may perform PSA on a specific reactor without taking into account the applicability of generic reliability data, and suspicion about such assessments raised because of the absence of plant-specific reliability data. To remove this doubt, a study has investigated the applicability of generic reliability. It has been shown that reliability data from various sources does not distort the results of PSA if they are utilized in performing PSA for a specific reactor. [20]

In that study, a number of reliability data sets extracted from different sources were analyzed. The subsequent analysis evaluates a fault tree (FT) for a specific reactor, using a number of reliability data sets and demonstrates the variances in the results. Furthermore, a comparison is performed with a procedural analysis utilizing ranges of reliability data. The results revealed that the PSA for a specific reactor employing reliability data which are taken from different sources is acceptable.

The variances are slight for the majority of components, only a few crucial components should be given more attention and further study. In the time being, the lack of specific reliability data should not be a barrier for performing a PSA on a specific reactor. [20] However, it is better to attempt to get plant-specific reliability data to fully remove all doubts about their applicability. Nevertheless, in the meantime the absence of novel reactor specific reliability data should not be a barrier to conduct a PSA to improve plant safety, mainly when main initiating events are to be found out. In any situation, it is strongly recommended for the analyst who faces a lack of data to identify the main components in the system to pay them more attention. [21] For novel components or components with no operational experience, generic data for similar components are considered with supplementary reliability evaluations, manufacturers' information and expert judgment. [18]

2.4. Common Cause Failure (CCF)

CCFs are being considered as one of the most critical matters in the development of PSA, particularly within FT modeling. A growing number of studies to reliability and safety analyses of

systems taking into account impact of CCF, considering the CCF uncertainties, valuation of CCF rates, are being introduced. In recent years, CCF have been an ongoing issue of investigation and arguments. Thus, CCFs have been given a great consideration within the PSA of NPPs. [22]

For a PSA, CCF data is generally extracted from existing operating experience issued by internationally available sources such as (IAEA) and (NUREG). Generic values may also be viable if it is considered that the available data is not relevant for the selected CCF group. Because there are generally no large inconsistencies between CCF parameters taken from different sources, this approach is acceptable in principle. However, it has to be traceable and documented.

Regarding the classification of CCF families, PSA applies assumptions in order to define the groups that contain redundant components for which CCF contributions should be considered. However, the assumption of complete diversification of certain redundant components (where it is assumed that CCF is not possible) has to be justified by a comprehensive analysis. This investigation has to cover all the CCFs and mechanisms (type, environment, manufacturer, maintenance, etc.) along with the long-term characteristics of these situations over the plant lifetime. This issue refers essentially to components of similar type, but made by different manufacturers, for cases where parts might be supplied by the same manufacturer or for components within a common maintenance program. Spare parts or maintenance materials may have an influence. Sensitivity studies will be useful in order to find out the potential CCF families for which thorough studies may be required. [10] It is a common practice not to model inter-system CCFs for existing plants because they are supposed to be insignificant contributors to large early release frequency, core damage frequency (CDF), etc. Nevertheless, for prospective reactors with inherent safety features needing to show compliance with reduced safety target values, special attention needs to be given to inter-system CCFs and CCFs associated with similarity in active sub-components (circuit breakers, motors, etc.). [23]

2.5. Modeling of Novel Design Features

Generally, in the PSA for novel reactors, the innovative design features result in decreasing the core damage frequency (CDF). Some new initiating events will be recognized, primarily associated with inadvertent actuation of the new automatic actions. The effects of these actions should be analyzed. Additional evaluations might be required in order to ensure that new design features are sufficiently addressed. These might include, as examples, studies showing the appropriate utilizing of conservatism in defining PSA success criteria, the employment of bounding parameters for PSA sensitivity studies and supporting calculations, and testing actions to validate calculations.

2.6. Modeling of Preventive Maintenance

Generally, because technical specifications and preventive maintenance detailed procedures are not available in the design stage, assumptions are made on preventive maintenance and on corrective maintenance intervals. These assumptions are built chiefly on the anticipated technical specifications and on the engineering experience. This method is generally accepted for a design phase PSA. However, if the preventive maintenance is predicted during power operation, comprehensive maintenance information, chiefly related to the configuration management, might be requested with the aim of ensuring that the maintenance configuration risk is appropriately addressed in the PSA.

2.7. Technical Specifications

The surveillance requirements and the technical specifications are generally not available during the design phase. The aspects should be modeled as accurate as possible since the PSA can be further used to define “risk-optimized” technical specifications and surveillance requirements. [15] In parallel with validation of the PSA, some safety authorities assess the design phase technical specifications to confirm that they will maintain the plant design validity by ensuring that the plant will be operated with the predefined design conditions, and with equipment that is crucial for preventing accidents and mitigating the accidents consequences. In some cases, complete design information, allowable values, equipment selection or further information are required to establish the

basis for the technical specifications. These plant-specific values should be provided when a joint license application is submitted for a certain plant.

2.8. Human Reliability Analysis (HRA)

To make PSA more accurate, improving of human reliability analysis (HRA) is vital. Experience shows obviously that human interaction is one of the key contributors to operational disturbances and accidents. In a study, it was concluded that probability of human error has approximately 58% contribution to events leading to increasing in core damage frequency (CDF). [24] At the same time, humans can effect several components and systems and therefore present hidden coupling factors between systems. Consequently, a proper human error analysis is required even in the most reliable systems. [25]

Currently, the HRA approaches for the PSA for novel reactors are generally similar for the existing reactors PSA. These approaches are used to quantify the pre-accidental and post-accidental HRA. During the design stage, detailed accident procedures and the use of a simulator to enhance HRA quantification usually are not available. The HRA is often used to establish the operator plans for a variety of accident scenarios. Moreover, it is likely that the HRA qualitative and quantitative analyses will be used to help enhance the comprehensive simulator training scenarios and accident procedures. Current HRA approaches have to be improved due to the existed limitations including the lack of theoretical basis for human operators situation assessment, and lack of considerations on the interdependency between human operators and I&C systems. To solve these issues, new methods should be proposed for the quantitative safety assessment of human operators and I&C systems. [26]

In the future, the expanded application of HRA approaches is foreseen, as well as the wide spread use of simulators. The availability of detailed information of the accident procedures and the severe accident management guidelines is considered a vital issue by all innovative reactor project analysts.

2.9. Systems Interdependencies

The systems interdependencies represent a crucial point of the design of the new plants. The PSA is one of the most powerful tools to study the impact of different design solutions. Even if the complete design is not finalized, the interdependencies between the safety systems, i.e. functional dependencies or induced by the support systems (power supply, cooling, ventilation, I&C, etc.) should be modeled as detailed as possible, and conservative assumptions should be used if the information is not available. The omission of the dependency modeling, even the detailed design of support systems is not known, should be avoided. [15]

2.10. Modeling of Instrumentation and Control (I&C)

Digital I&C systems are the present design solution for innovative reactors. The many exclusive attributes of these systems, create challenges for PSA modeling. The main issues are the models ability to identify dependences created by digital I&C, specifically dependencies between an initiating event (such as a spurious signal) and failures of safety functions (theoretically, the FT modeling is a possible solution for this issue). The second issue concerns data, which is still challenging to find, particularly for software and CCFs. The digital I&C is not an exclusive issue to new plants, but due to higher safety expectations the role of I&C is growing and becoming a potential major issue. Even though there is no real practice consensus for the digital I&C modeling and quantification, some tentative methodologies are established and integrated in PSAs. [18]

2.11. External Hazards

The ability to identify the external hazards for the PSA is different for diverse new reactor projects. This is due to variations in the project development status, chiefly if the site is identified or not, and to the expected effect of the different external hazards on the prospective plant safety, which

depends on the country and the site. Generally, nowadays only a few hazards for PSA are recognized for new reactors. Many external hazards are addressed using analysis or other simplified approaches that approximate the hazards contribution to overall prospective plant risk. The prospective possible hazards evolution (prompted by climate change for example) are generally not explicitly considered in the analysis (however, climate change is sometimes taken into account in the external hazard analyses normally to include bounding assessments that are meant to show the margin of design for these hazards). The combinations of hazards, in addition to the induced internal hazards, seem to have not been analytically considered in the performed assessments. [18]

In order to allow the assessment of the influence of the internal and external hazards on the plant safety, it is important that the design phase PSA incorporates useful information (like equipment location, fire compartments, etc.), even using simplified assumptions. A thoughtful verification should be done regarding the possible common mode failures of redundant trains, systems or functions. [15]

2.12. Continuous Design Risk Monitoring

The conventional use of PSA within the design phase is centered on a continuous monitoring of the design against established conventional quantitative risk metrics such as CDF and various release frequencies. To be able to enter in this phase of the PSA support to the design, a somehow complete preliminary design needs to be reached. Depending on the design stage, an extremely simplified fault tree (FT) modeling of support systems is used. The complete, even though simplified, PSA model allows at this point for a more comprehensive risk monitoring of the design by tracking intersystem dependencies that cannot be easily tracked in a single failure criterion approach.

The risk-informed design approach Generation IV concepts suggests continuous interaction between the design team and the PSA team, with a more structured feedback from the PSA to the design side. In this approach, PSA results have a more direct influence on the plant design, rather then simply following its development.

The main "drawback" of such an approach is that probabilistic studies need to be initiated at a very early stage of the design, when several required design information may only be partially or qualitatively available. This requires a more flexible approach to probabilistic analysis than used in the past and, especially, results in a relevant number of assumptions, which importance in the risk assessment is well beyond what is currently handled in a PSA for operating plants. A fundamental part of using PSA in the initial design stage was therefore the documentation and monitoring of all these assumptions for further analysis and confirmation of their actual applicability. [16]

2.13. PSA Supporting Studies

Specific support studies are usually conducted for the new reactors PSAs. This typically includes studies such as: thermal hydraulic analyses and system engineering analyses for defining mitigating systems' success criteria. The necessity for developing specific studies is identified according to the PSA standards and guidance. The design basis reports and safety report analysis represent other sources of information for the new reactors PSA development, along with the PSA reports of similar reactors.

2.14. Interpretation of PSA Results for New Plants

There are a number of ways that the results of the PSA are used to evaluate the design of a new plant, to identify the design weaknesses and to assess and rank potential alternatives for enhancing the design. Generally, these include:

- Safety metrics/indicators such as safety system reliability, core damage frequency, large early release frequency, etc. Safety metrics/indicators show whether the overall risk from the plant is low enough to start a license process.

- Lists of minimal cut-sets. The integrated list of top minimal cut-sets and lists of minimal cutsets generated for separate initiating event groups for different plant operating modes are reviewed. Both internal initiators and hazard-induced initiating events are considered. If a single order minimal cut-set representing an independent failure, e.g. a failure of a common support system component, appears in the list of minimal cut-sets provided within the internal event PSA, then, hence, the single failure criterion is not met, and redundancy of the system concerned has to be increased. If a similar finding is found in the internal hazard (e.g., fires and floods) PSA, then separation and segregation of safety related components is insufficient and needs to be improved.

- Importance functions for basic events, sets of basic events, sets of initiating event and safety systems. High importance of an independent failure event might be an indication of insufficient redundancy in some plant operating modes and the necessity for enhancement. In this situation, either system redundancy requires to be improved or limiting conditions for system operation should become tougher for this particular plant operating mode, if possible. High importance of a CCF could be an indicating of insufficient diversity to some safety functions. In this situation, a significant change in the basis of design might be required. High importance of a human error may indicate a poor man machine interface. Increasing automation of the plant can be considered as an additional design measure in this case.

These results are used to decide whether the proposed design is balanced or there is a need for additional measures to be integrated to reduce risk. The results of the PSA are being used as one of the inputs to a process of risk informed decision making respecting to the option to be incorporated into the design. The PSA is used to estimate the reduction in the risk for each of the options identified. [23]

3. FUTURE DEVELOPMENTS AND RESEARCH

While the PSA methodology is reasonably robust in most areas, additional research is needed and is in progress in several areas. In some cases this research is conducted to improve the efficiency of the PSA process. In other cases, it is performed to reduce the uncertainties associated with PSA results, thus making it easier to use the results and analyses in a regulatory environment or to change operational practices. Several activities are related to the development of new or advanced reactors.

Key areas of research in progress include the following: Development of PSA methods; PSA for internal and external hazards; Common cause failure (CCF) modeling; Human reliability analysis (HRA); Reliability data collection; PSA for passive systems; Reliability of digital systems; Level 2 and Level 3 PSAs; Uncertainties; Dynamic PSA; Modeling of ageing in PSA; Fuel route PSA; and Use of PSA in risk-informed decision making (RIDM).

It can be seen that the general areas of PSA research are not really new, but in each area substantial activities are ongoing. Of special note is research relating to severe accidents, to fire, and to human factors, which supports improved PSA modeling. Moreover, research relevant to problems relating to new plants (e.g., digital I&C and passive systems) is receiving high priority. [27] To improve the quality of the PSA, the following areas are suggested for future studies:

- Develop a systematic approach to estimate the reliability of a newly introduced system or component for the novel reactor.

- Establish a methodology for evaluating the reliability of a digital I&C in passive safety systems.

- Develop a methodology for estimating the CCF data of a newly introduced component.

- Establish a structural framework for HRA activities for novel reactor designs.

4. CONCLUSION

The use of the PSA from the early design for Generation IV reactors shows that the PSA is a very valuable tool to obtain an optimized and balanced design by taking into account the information provided by the risk assessment. On the other hand, the development and the use of PSA should take into account some specific methodological aspects of a design phase PSA. The decision making process should consider the fact that PSA for a novel plant concept may have substantial uncertainties. Extensive sensitivity studies should be performed and the uncertainties should be known and taken into account. [28]

In many engineering design activities, the use of PSA methodology is now accepted, but with controversy in some technical aspects. The main concern is with the misconception that PSA methodology is considered as a tool to conduct a 'risk study' only and not as a comprehensive 'probabilistic tool' for predicting the system design behavior and to optimize it respecting various goals (e.g. investment, safety, reliability, availability).

Modern designs typically consist of active and passive systems, controlled by computers and supervised by plant staffs. Therefore the PSA methodology need to be enhanced for considering in a proper way the passive components and computer software and hardware. It makes no sense if a system design is assessed by "traditional" PSA methodology and the effect of the computer system, which controls the system, is neglected. In this framework there exists a challenge for enhancing the models and the database in PSA methodology today.

For the new reactors, the PSA is being accepted as one of the key methodologies to justify safety-critical features in the conceptual and preliminary design phase and to address new operation conceptions. However, there still remain some aspects related to PSA in order to better consider the innovative reactors specific features. Most of the identified PSA matters are well recognized. Also, most of the subjects are relevant to all types of reactors in the design stage. However, there obviously are greater challenges in dealing with these matters when the plant is in the conceptual design stage (and complete design specifications have not yet been set).

REFERENCES

[1] *"Basis for the Safety Approach for the Design & the Assessment of Generation IV",* Nuclear Systems, Generation IV International Forum (GIF) Risk and Safety Working Group (RSWG), Revision 1, GIF/RSWG/2007/002, The OECD Nuclear Energy Agency, November (2008).

[2] *"Proposal for a Technology-Neutral Safety Approach for New Reactor Designs",* International Atomic Energy Agency (IAEA), IAEA-TECDOC-1570, September 2007, Vienna.

[3] F. Bertrand, *"Risk-informed analysis as a support to the preliminary design of the CEA GFR2400"*, Workshop on PSA for New and Advanced Reactors, OECD Conference Centre Paris, France, NEA/CSNI/R(2012)2, pp. 85-95, July (2012).

[4] C. Bassi et al., "Level 1 probabilistic safety assessment to support the design of the CEA 2400 MWth gas-cooled fast reactor", Nuclear Engineering and Design 240, pp. 3758–3780, (2010).

[5] K. Kurisaka, "Probabilistic Safety Assessment of Japanese Sodium Cooled Fast Reactor in Conceptual Design Stage", 15th Pacific Basin Nuclear Conference, Sydney, Australia, (2006).

[6] T. W. Kim et al., "Preliminary Level 1 PSA Results for SFR-600 Conceptual Design", Proceedings of the 18th International Conference on Nuclear Engineering ICONE18, ICONE18-30367, Xi'an, China, (2010).

[7] P. F. Nelson et al., "A design-phase PSA of a nuclear-powered hydrogen plant", Nuclear Engineering and Design 237, pp. 219–229, (2007).

[8] Yu. V. Shvyryaev et al., "Use of Probabilistic Analysis in Safety Validation of AES-2006 designed for the Novovoronezh Nuclear Power Plant Site", Atomic Energy 106, No. 3, (2009).

[9] J. Tong et al., "Development of Probabilistic Safety Assessment with respect to the first demonstration nuclear power plant of high temperature gas cooled reactor in China", Nuclear Engineering and Design, 251, pp. 385–390, (2012).

[10] M. H. PSAsad et al., "Level-1, -2 and -3 PSA for AHWR", Nuclear Engineering and Design, 241, pp. 3256– 3269, (2011).

[11] J. H. Lee et al., "Safety system consideration of a supercritical-water cooled fast reactor with simplified PSA", Reliability Engineering and System Safety, 64, pp. 327–338, (1999).

[12] H. Yamano et al., "Development of technical basis in the initiating and transition phases of unprotected events for Level-2 PSA methodology in sodium-cooled fast reactors", Nuclear Engineering and Design, 249, pp. 212– 227, (2012).

[13] "Workshop on PSA for New and Advanced Reactors", OECD Conference Centre Paris, Nuclear Energy Agency (NEA), NEA/CSNI/R(2012)2, July (2012).

[14] Kamiar Jamali, "Use of risk measures in design and licensing of future reactors", Reliability Engineering and System Safety 95, pp. 935–943, (2010).

[15] G. Georgescu et al., "Use of PSA at Institute for Radiological Protection and Nuclear Safety for EPR licensing purposes", Institute for Radiological Protection and Nuclear Safety (IRSN), Fontenay aux Roses, France.

[16] A. Maioli et al., "Use of PSA in the Development of SMRs, Workshop on PSA for New and Advanced Reactors", Workshop on PSA for New and Advanced Reactors, OECD Conference Centre Paris, NEA/CSNI/R(2012)2, pp. 241-261, July (2012).

[17] "Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants", International Atomic Energy Agency (IAEA), IAEA-TECDOC-1511, July 2006, Vienna.

[18] "A Joint Report on PSA for New and Advanced Reactors", Nuclear Energy Agency (NEA), NEA/CSNI/R(2012)17, (2012).

[19] G. Georgescu and F. Corenwinder, "Lessons learned from IRSN review of Flamanville 3 Level 1 PSA, Workshop on PSA for New and Advanced Reactors", OECD Conference Centre Paris, France, NEA/CSNI/R(2012)2, July (2012).

[20] Jia Ning, "Applicability Analysis of Generic Reliability Data for PSA on a Specific Reactor", 18th International Conference on Nuclear Engineering: Volume 3, Xi'an, China, 17–21 May, (2010).

[21] Ulrich Hauptmanns, "The Impact of Reliability Data on Probabilistic Safety Calculations", Journal of Loss Prevention in the Process Industries 21, pp. 38–49, (2008).

[22] Duško Kančeva and Marko Čepinb, "A New Method for Explicit Modeling of Single Failure Event within Different Common Cause Failure Groups", Reliability Engineering and System Safety 103, pp. 84–93, (2012).

[23] V. Morozov and G. Tokmachev, "Lessons Learnt from PSAs for New and Advanced Reactors in Russia", Workshop on PSA for New and Advanced Reactors, OECD Conference Centre Paris, France, NEA/CSNI/R(2012)2, July (2012).

[24] In YH, "*Key risk concepts, in: Proceedings of the IAEA workshop on improvement of safety and economics of NPP"*, Daejeon, Korea, (2002).

[25] Pekka Pyy and Bjorn Wahlstrom, *"Modeling the Human in PSA Studies*", Reliability Engineering and System Safety 22, pp. 277-294, (1988).

[26] Man Cheol Kim and Poong Hyun Seong, "*A Computational Method for Probabilistic Safety Assessment of I&C Systems and Human Operators in Nuclear Power Plants",* Reliability Engineering and System Safety 91, pp. 580–593, (2006).

[27] *"Use and Development of Probabilistic Safety Assessment: An Overview of the situation at the end of 2010"*, Nuclear Energy Agency (NEA), NEA/CSNI/R(2012)11, (2013).

[28] Gabriel Georgescu et al., *"Use of PSA at Institute for Radiological Protection and Nuclear Safety for EPR licensing purposes"*, Institute for Radiological Protection and Nuclear Safety (IRSN), Fontenay aux Roses, France.