Risk-Informed Approach to Functional Safety Assessment of Instrumentation and Control Systems of Reactor Protection Systems – A Systematic Mapping Study

A.S. Korolev, A.A. Tribelev

Abstract – The safety of nuclear power plants (NPPs) is achieved through the implementation of a multi-layered protection system and safety functions, tailored to the configuration of the nuclear facility. One of the critical systems in ensuring safety is the reactor protection system, which ensures the automatic transition of the reactor to a controlled safe state during emergency situations and in the event of deviations from normal operating conditions. An effective assessment of the functional safety of reactor protection systems during the design, implementation, and operation phases serves as a vital tool for confirming compliance with safety requirements and ensuring reliable protection of NPPs.

In contemporary contexts, the evaluation of functional safety effectiveness is conducted based on a risk-oriented approach, which is implemented in accordance with the regulatory requirements set forth by the IAEA and national regulatory bodies.

This article presents a systematic study that investigates the risk-oriented approach to assessing the functional safety of reactor protection systems in NPPs. The research is grounded in a systematic mapping of findings from a sample of 72 articles, selected according to predefined criteria. Consequently, the current state of the field has been defined, and key methodologies, methods, and tools have been identified. Additionally, significant trends have been highlighted, including the integration of modern modeling techniques with traditional approaches. Furthermore, areas for growth and promising directions for future research have been identified, as noted in the reviewed articles.

***Keywords*— Risk-Informed Approach, Nuclear Power Plants, safety assessment.**

I. Introduction

The safety of NPPs is a paramount concern. Its implementation necessitates a multi-layered protection system aimed at preventing accidents and mitigating their consequences [1]. Reactor protection systems play a crucial role in maintaining the safety of NPPs by ensuring the automatic transition of the reactor to a safe state during emergency conditions and activating safety systems in the event of deviations from normal operating conditions. The execution of functions within reactor protection systems, which are essential for maintaining safety, must comply with the requirements set forth in regulatory documents [2, 3], which establish guidelines for the development, verification, and validation of safety-critical instrumentation and control systems. An effective assessment of the functional safety of reactor protection systems is an important tool for confirming compliance with safety requirements and ensuring reliable protection of NPPs.

In contemporary contexts, the evaluation of functional safety effectiveness is conducted based on a risk-oriented approach. This approach is implemented in accordance with the recommendations [4] and the requirements of regulatory documentation [5, 6]. Safety justification is built on an integrated approach that encompasses PSA and deterministic methods for risk identification, risk assessment, and scenario determination. Such an approach allows for a more accurate evaluation of the NPP configuration as a whole and the control systems in particular, ensuring an adequate level of safety and compliance with regulatory requirements [7]. The application of a risk-oriented approach facilitates more informed decision-making during the design and operation of NPPs, minimizing potential risks and ensuring reliable reactor protection.

Despite the comprehensiveness of the methodological recommendations outlined in the IAEA Guides, as well as the existence of a regulatory framework that collectively supports approaches to assessing the justification of functional safety in reactor protection systems, the application of a risk-oriented approach in this field reveals noticeable areas for development. Based on conclusions drawn from existing assessment practices [8], the practical implementation of these approaches contains an element of dependence on expertise, which may amplify the factor of subjectivity in the decision-making process. Furthermore, the established practice of implementing a risk-oriented approach based on probabilistic models, in accordance with the requirements of [7], incorporates elements of both probabilistic and deterministic approaches, which can also lead to vulnerabilities in the selection of considered scenarios and, consequently, potentially result in an incomplete assessment of risks associated with the functioning of reactor protection systems. This trend is also noted in [8]. The calculation of a complete set of scenarios and dependencies significantly increases the cost of safety design. Additionally, it is important to note that the design of safety models is based on accumulated reliability data for system components, particularly concerning new technologies and digital systems, which can complicate the

Manuscript received July XX, 2025. This work was supported in part by the National Research Nuclear University MEPhI Higher Engineering School.

A.S. Korolev is with the RTU MIREA, korolev@mirea.ru

A. A. Tribelev is with the NRNU MEPhI HES, *e-mail: AATribelev@mephi.ru.

application of classical methods in this field, such as Fault Tree Analysis (FTA) or Failure Mode and Effects Analysis (FMEA), or render them limited due to incomplete data. The aforementioned aspects indicate specific areas for improvement in assessment approaches through systematic research and the exploration of enhancement pathways, which will enable a more effective application of the risk-oriented model of functional safety in reactor protection systems. This can be further strengthened by the positive effects resulting from the implementation of new measures for the digitalization of the nuclear industry [9]

This research paper is structured as follows. In Section II we present the applied research methods including the research questions studied and the sources of data for search. In section III we present the results of mapping study

II. RESEARCH METHOD

The objective of the research presented in this article is to identify topics related to the methodology, methods and tools used for the development, analysis and assessment of safety and reliability concerning risk-oriented approaches to reactor protection systems. This includes the extraction of metadata to formalize conclusions, explore research prospects and identify limitations noted in the studies of the authors. To conduct a literature review in this context, we will employ the method proposed by Peterson – a systematic mapping study described in [10]. A systematic mapping study aims to provide an overview of existing publications and literature in the area of interest. In the context of the objectives set forth by the current research, conducting such a review may help identify avenues for further investigation and assess the quality of existing studies.

A. Research questions

RQ.1 How is the functional safety assessment of reactor protection systems (RPS) in NPPs represented in the published literature?

This research question aims to determine the understanding of how the assessment of the implementation of functional safety in reactor protection systems is addressed in existing studies. Primarily, it is important to ascertain whether the literature encompasses modeling of the subject area related to the assessment of functional safety in reactor protection systems or focuses on the direct implementation of safety functions during the deployment of reactor protection systems in NPPS. Based on the metadata defined for this question, it will be possible to identify the prevailing methodologies, methods, and tools utilized in the examined field. Another aspect of this research is to ascertain how the literature documents the approach to assessing the implementation of functional safety in reactor protection systems in NPPs. The answer to this question will enable a clear formalization of the current state of research in the selected area.

RQ.2 Which topics are covered regarding functional safety assessment of RPS in NPP?

This research question will help identify which research and practical aspects related to ensuring functional safety in reactor protection systems in NPPs are addressed in the publications. The analysis of existing publications aims to uncover the methodologies and methods employed in risk-oriented modeling and management within the selected subject area. Additionally, the study will examine approaches to justifying compliance with criteria regulated by IAEA recommendations and requirements outlined in regulatory documentation. Furthermore, this inquiry will consider approaches to maintaining the functional safety of existing safety systems in NPPs.

RQ.3 Which evaluation methods are applied by the authors of papers in the list of primary studies?

The objective of this research question is to systematically define and classify the assessment methods employed by authors of studies that fall under the criteria of the analyzed sample. This analysis aims to identify the methodological approaches used for the collection, processing, and interpretation of data that define the parameterization of functional safety in reactor protection systems in NPPs. The analysis of the associated tools includes the identification of specific aspects of practical implementation (such as software, models, simulations, etc.) utilized in the assessment process. The outcome of this inquiry will be the construction of a comprehensive picture of the methodological landscape in the studied field, allowing for the evaluation of the rigor and reliability of the presented evidence, the identification of gaps and limitations, and the exploration of promising approaches and research directions.

B. Data sources and research Strategy

We utilized the following databases for our search.

- IEEE Xplore Digital Library
- Science Direct
- Web of Science
- Scopus

A search for scientific articles presented at conferences and published in academic journals was conducted using these knowledge bases.

As part of this search, a query was conducted followed by the selection of studies related to the implementation of a risk-oriented approach to the assessment of functional safety in reactor protection systems.

The search query is as follows:

("Risk informed approach" or "Probabilistic safety assessment") AND ("functional safety" OR “IEC 61513”) AND (“Nuclear Power plant” OR "Nuclear facility" OR "nuclear energy objects") AND ("I&C" OR "Reactor protection system").

In the body of the query, the first part formalizes a probabilistic request for conducting an assessment. The second part of the search query specifies the application domain of the probabilistic modeling approach. To enhance the query, the primary standard [3] relevant to this field was included in the request in cases where the article does not directly justify the use of the term "functional safety." The third part of the query formalizes the object of nuclear energy utilization for which PSA is applied. The fourth part of the query specifies the system within the instrumentation and control systems that is subject to analysis. Here, to strengthen the search, the general term "Instrumentation and control system" was included alongside the specific term "reactor protection system." The last two assumptions are based on the fact that such strict terminology may not always be applicable. Additionally, consideration may be given not

only to power reactors but also to research reactors. The search was conducted across titles, abstracts, and full texts of the selected works. The work itself may be dedicated to highly specialized tools used in this field, such as the application of specific software to solve particular tasks. Consequently, the high-level metadata may not contain the required answer to the query. Nevertheless, the methodology contained in such an article can be scaled for application in the broader research area.

C. Study Selection Criteria

During the search, a syntactic match between the query and the search topics was obtained. As a result, a large number of articles directly or indirectly related to the research area of this work were found. The following criteria were established:

1. Inclusion Criteria:

IC1. Scientific articles that discuss probabilistic safety justification;

IC2. Scientific articles that examine methodologies considered for probabilistic safety justification in the context of integration with other methodologies;

IC3. Scientific articles that address specialized tools for safety proof based on a probabilistic approach for specific tasks, which can also be scaled to the entire studied area;

2. Exclusion Criteria:

EC1. Scientific articles published prior to 2005, as a "snapshot" of the current state of the research direction is required.

EC2. Technical reports, as they contain a limited amount of metadata that can be used for analysis;

EC3. Articles where the probabilistic safety model is mentioned indirectly, and the article itself is not dedicated to the selected issue;

D. Study Selection Process

The process of selecting studies for this systematic mapping review was carried out in several stages. The initial sample included 623 articles. This volume was subjected to filtering based on the predefined inclusion and exclusion criteria. The inclusion criteria (IC1-IC3) focused on scientific publications addressing issues of probabilistic safety justification, the methodology for integrating probabilistic approaches with other safety assessment methodologies, as well as specialized tools applicable to solving specific tasks within the studied area. The exclusion criteria (EC1-EC3) allowed for the elimination of publications that did not align with the objectives of the research. The exclusion was conducted in stages, in accordance with the descriptions of the relevant criteria. As a result, 72 articles were selected from the initial sample [11-83], which were included in the final analysis. This selection allowed for the formation of a representative "snapshot" of the current state of research in the application of a risk-oriented approach to the assessment of functional safety in reactor protection systems.

E. Data Extraction

Based on the obtained sample, a tabular database was created for further work with the metadata. In the course of working with the metadata, primary information related to common aspects across all articles and secondary information related to the search queries was processed. All studies that passed through the filtering based on the criteria were examined and analyzed. From this, information was synthesized. The following information was included in the database:

Author's name;

Year of publication;

Title of the article;

Abstract of the scientific article;

Conclusion of the scientific article;

Methodology for assessing the functional safety of reactor protection systems presented in the article (RQ1).

Specific methods used for assessing the functional safety of reactor protection systems (RQ1).

Aspects of functional safety of reactor protection systems addressed in the study (e.g., reliability, availability, maintainability) (RQ2).

Applicable standards and regulations in the context of assessing the functional safety of reactor protection systems (RQ2).

Key trends in research related to the assessment of functional safety of reactor protection systems (e.g., application of new technologies) (RQ2Limitations noted by the authors regarding the methods used and the results obtained (RQ3)

Methods applied for evaluating the presented approaches and results (e.g., modeling, sensitivity analysis, expert assessment) (RQ3).

III. RESULTS

In this section, the results of the conducted study based on the analysis of [11-83] included in the final sample according to the selection criteria are presented.

Figure 1 shows the distribution of publications by year. As can be seen, the peak of research publication results occurs in 2016, 2020, and 2022, with more than 10 publications per year. Despite local minima observed in certain years, there is an overall cyclical growth trend.

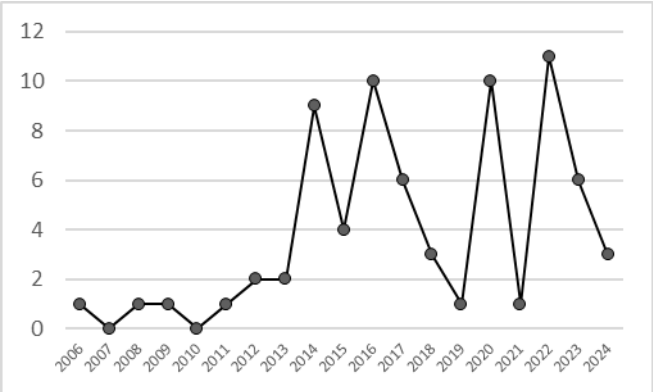

Figure 1 – Distribution of Research by Year

Additionally, based on the preliminary analysis, conclusions can be formalized regarding the previously defined search queries.

RQ1. How is the functional safety assessment of RPS in NPPs represented in the published literature?

The representation of studies on the assessment of functional safety of reactor protection systems within the selected literature is characterized by a diversity of approaches and research directions that cover various aspects of the lifecycle, analysis, and optimization of systems. In addressing the first query, the following types of formalization can be highlighted.

The first group of studies is related to modeling and reliability analysis. Here, general approaches to modeling can be identified [16, 17, 20, 26, 35, 43, 47, 51], which are associated with classical methods for working with the reliability of complex systems, such as FTA, Markov networks, Bayesian trust networks, and dynamic modeling [17, 43, 47]. These methods take into account temporal dependencies, modeling failures due to common causes [16, 47], justifications for software implementation assessments for digital I&C [12, 35, 49, 60, 62], and the integration of human factor assessments into the overall safety model [15, 35].

The second group of studies can be identified as focusing on technological aspects and architectural approaches. Within this group, the examination of so-called field programmable gate arrays (FPGAs) for the implementation of RPS and subsequent processes of verification and validation can be highlighted. This approach is discussed in [14, 19, 52]. Additionally, this group includes research on the implementation of redundancy architecture from the perspective of safety and availability, as presented in [22].

Another group consists of studies that explore methods for optimizing and enhancing the safety of existing systems. Two directions can be distinguished here. The first involves investigating the assumption of using a risk-oriented approach to identify critical components of RPS, followed by their assessment and systematic identification of potential safety improvements. This is suggested in publications [11, 30, 31]. This approach aims to improve the configuration of the instrumentation and control (I&C) systems responsible for safety. On the other hand, a pathway is proposed for maintaining the state [21], or an approach related to self-diagnosis [55].

Another identified group of studies focuses on the examination of safety analysis methods. Within this group, two major directions can be distinguished. The first is FTA, which is related to the expertise of fault trees for formal specifications of RPS requirements [24]. The second direction involves system-theoretic process analysis (STPA) for identifying unsafe control actions in protection systems [29, 44, 68].

As evident from the brief preliminary analysis, there is a trend towards transitioning from classical and simpler methods to more complex and dynamic approaches. Additionally, a second trend is noted regarding the optimization of existing I&C solutions that are part of the RPS framework.

RQ.2 Which topics are covered regarding functional safety assessment of RPS in NPP?

Within this research question, it was planned to determine which research and practical aspects related to ensuring functional safety in nuclear reactor protection systems are covered in the publications. After conducting a preliminary analysis of the selected body of research, the following themes can be highlighted.

The most extensive theme for study is the methodology of reliability analysis and safety justification, which includes large groups for examination such as PSA, risk assessments, and a systematic approach to justifying selected decisions [11, 31, 17, 29, 35, 39, 43, 44, 45, 47, 48, 56, 57, 58, 80].

Another significant theme for discussion is the direct implementation. This topic includes descriptions of approaches to practical reliability analysis of digital modules, programmable controllers, and comprehensive architectural considerations [13, 14, 16, 17, 18, 19, 20, 22, 35, 40, 41, 49, 51, 62, 65, 67, 73].

Another important theme is the implementation of software for RPS components. This involves examining the complete lifecycle of such development, from design to system reliability analysis during the verification and validation stages of software components [16, 22, 30, 31, 32, 35, 37, 40, 46, 49, 50, 52, 53, 61, 62, 68].

A large thematic group can also be identified that is related to the support of operation, including hypotheses about possible strategies [21, 28, 30, 31, 46, 69].

Additionally, there are slightly less covered themes in the overall body of research, but nonetheless important from the perspective of further studying the issues in the chosen field. These include improvements in Human Reliability Analysis (HRA) and Human-Machine Interaction (HMI) [15, 33, 35]. There is also a hypothesis regarding the application of AI technology in conjunction with classical methods [23].

RQ.3 Which evaluation methods are applied by the authors of papers in the list of primary studies?

In the context of studying the response to this question, a map of methods was created, which are considered by the authors as methods for assessing and analyzing the safety of RPS. The generalized distribution of the identified methods is presented in Figure 2.

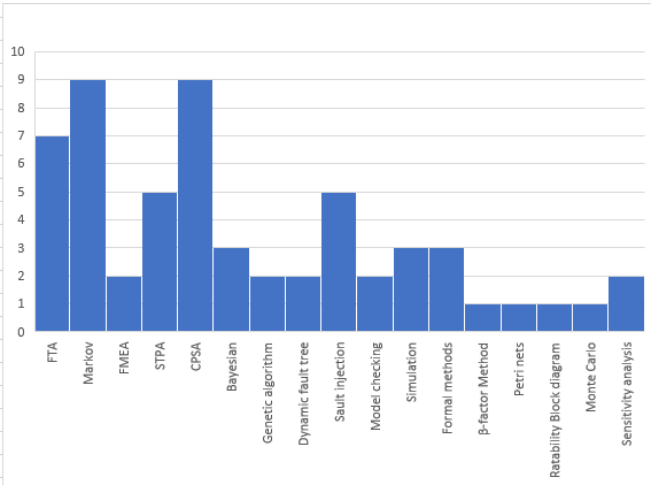

Figure 2 – distribution of assessment methods in research

Distribution of assessment methods in research The authors consider the following methods as techniques for assessing and analyzing the safety of RPS: FTA [12, 17, 35, 42, 47, 70, 76] for determining failure probabilities and identifying vulnerabilities in the system, Markov state-transition models

[12, 17, 22, 39, 43, 45, 51, 70, 74] for modeling system dynamics, including failure states, fault detection, and recovery, Ratability Block diagram [34] for quantitative assessment of the unreliability of I&C configurations, fault mode and effects analysis [22, 44] for identifying potential failures, their consequences, and mitigation strategies, STPA [25, 29, 44, 68], for identifying unsafe control actions, software fault tree analysis (SFTA) [24], for analyzing software requirement, comprehensive PSA [11, 21, 35, 40, 47, 48, 49, 62, 70], including the assessment of failure probabilities on demand and false alarm probabilities, Bayesian belief network [26, 31, 62], for improving the reliability of RPS, Multi-objective genetic algorithm [46, 60], for optimizing system design while considering safety, reliability, and cost requirements, Mont Carlo Methods [34], sensitivity analysis [30, 31] , dynamic fault tree [73, 76], dynamic flowgraph methodology [76], hazard and operability analysis (HAZOP) [57], fault injection [77, 80, 81, 82, 83], model checking [58, 75], simulation [53, 58, 75], formal verification [57, 66, 75], β-factor Method [79], timed Petri nets [65].

IV. ANALYSIS AND DISCUSSION

The content of this section implies a deeper analysis and subsequent discussion of the results obtained from the publications that meet the selection criteria [11-83]. The chosen topic is not entirely new, but it has been gaining traction and development in recent times.

A. Main research directions

The conducted analysis of the information presented in the literature has identified several key research directions concerning risk-oriented assessment of functional safety in reactor protection systems. Significant attention is devoted to justifying approaches to modeling and analyzing the reliability of digital Instrumentation and Control (I&C) systems. These processes incorporate operational aspects such as repair time, testing frequency, self-diagnostic properties, and the impact of selected architectural solutions. When designing these approaches, associated challenges are considered, such as the so-called "curse of dimensionality" in modeling complex systems and the development of mitigating methods to reduce its impact. Another property examined during the design phase is cybersecurity in the context of reliability and safety. All these approaches are analyzed both in a static state and with consideration of temporal parameters, which serves as a basis for justifying operational support strategies.

Another important research theme is the assessment and enhancement of the reliability of digital I&C systems through the development and refinement of reliability models that account for failures of various natures (hardware, common cause failures, software, etc.). These models also integrate results from the previous theme to improve reliability management outcomes while considering temporal parameters.

The reviewed studies emphasize the importance of utilizing automated tools and environments for conducting verification and validation procedures of implemented solutions. This approach is considered in conjunction with the unification of formal methods in the specification of requirements, analysis results, and verification as foundational data for subsequent steps. Additionally, the use of simulation-based testing methods for robustness verification is proposed. This approach involves working with a hybrid model that combines traditional methods (e.g., FTA, Markov Modeling, etc.) with modern approaches (e.g., fault injection, machine learning, etc.). The use of automation tools for preparing input data is also suggested..

A related theme, sharing similar implementation approaches, is the safety verification of software for reactor protection systems. Here, trends towards the application of formal methods for the specification, analysis, verification, and validation of the software itself can be identified. The application of formal methods, languages, and tools (e.g., NuSCR, SFTA, etc.) for correctness and safety verification is considered. Further integration of results into the overall assessment methodology is carried out based on FPGA approaches, including the development of testing and self-diagnostic methods. Based on these assumptions, principles can be established to reduce the occurrence of common cause failures. Additionally, the application of safety cases for the assessment and demonstration of the safety and reliability of complex software systems is discussed.

Management of the design and optimization of implemented architectures is also a subject of research. Special attention is given to justifying compliance with [5]. This includes the implementation of functional safety management processes throughout the entire lifecycle of I&C, defining, justifying, and proving the achievement of required safety integrity levels (SIL). Based on general requirements and classical solutions, hybrid (analog-digital) architectures are considered to enhance system resilience against common cause failures, as well as the exploration of new design approaches (e.g., "Forward Design").

Another theme is the improvement of human-machine interfaces to mitigate the influence of human factors. Research in this area is based on human reliability analysis (HRA) approaches. This includes investigating the impact of digital human-machine interfaces (HMI) on operator behavior and developing models that account for cognitive aspects of operator activities in non-standard situations. Studies also explore the development of operator support tools that enable operators to effectively monitor and operating NPPs, particularly in emergency situations, and develop HRA models that consider cognitive aspects of operator activities in non-standard situations and the influence of digital interfaces.

Furthermore, the reviewed studies highlight the necessity of applying methods and tools for analyzing error propagation in I&C systems. This aspect is linked to the optimization of the design of control and instrumentation systems, especially in the context of cost and performance constraints. This includes the exploration of multi-criteria optimization methods using genetic algorithms to achieve an optimal balance between safety, reliability, and cost considerations. Finally, the research acknowledges the importance of assessing the impact of aging and degradation of components on the reliability of I&C systems, underscoring the need for developing strategies to mitigate these effects and ensure the long-term performance and safety of the system.

B. Assessment methods

As methodologies and methods for the correct implementation of a risk-oriented safety model, researchers have considered quantitative, qualitative, formal, and modeling-based approaches.

In accordance with the stringent boundary conditions defined by regulatory requirements [2,87], the primary proof tools are represented by quantitative methods. Among these, the multi-level PSA is primarily used for overall risk assessment. This methodology involves the use of classical proof methods (FTA, FMEA, Markov Modeling) to identify and quantitatively assess potential failure scenarios. Additionally, simulation modeling methods are employed to determine system behavior under various conditions and to evaluate probabilistic outcomes. In the context of simulation modeling, the authors also consider dynamic analysis methods (e.g., DFM or SCM), which allow for the modeling of system behavior over time and under changing conditions. These approaches are used in conjunction with static state approaches, such as finite element methods for analyzing structural integrity and component behavior. In this context, to alleviate some of the conservatism of the approaches, the authors propose the possibility of integrating machine learning methods with classical approaches.

Another approach defines qualitative safety assessment methods. Several implementation directions are identified here. FMEA is used for the systematic identification of potential failure modes and their consequences, while HAZOP is employed to identify potential deviations from intended operating conditions and associated hazards. STPA provides a more comprehensive, systemic approach to hazard analysis. The Safety Case methodology is utilized as a structured approach for demonstrating and documenting arguments in favor of the safety of complex systems.

The authors also emphasize the importance of formal methods as proof tools. These methods are based on formal specification of requirements (e.g., using NuSCR or Z-notation) followed by rigorous verification using techniques such as Model Checking and Abstract Interpretation.

Specific modeling methods identified in the studies include models based on beta distribution functions, time-stamped Petri nets for analyzing temporal loops, and UVM-SystemC for co-simulation of hardware and software. In the area of testing, there is a focus on the quantitative assessment of the throughput of Function Block Diagrams (FBD) and the use of statistical methods for practical evaluation of safety-critical software. Regarding cybersecurity assessment, STPA and related approaches are highlighted for identifying security vulnerabilities and evaluating their impact on system safety.

The most frequently used methods reported in the reviewed literature include mathematical modeling and the calculation of probabilistic characteristics. Experimental methods, including laboratory testing and simulation of emergency situations, are employed to validate models and assess system behavior under extreme conditions. Simulation modeling using computer models is widely used to simulate system behavior under various operating conditions and failure scenarios. Formal verification is utilized for mathematical proof of software correctness and its compliance with safety requirements. Finally, heuristic methods that employ expert judgments, analogies, and other knowledge-based approaches are used to complement other analytical methods.

C. The context under consideration

All the aforementioned approaches are examined in the context of their application to aspects of functional safety. Primarily, the provided toolkit is utilized to demonstrate the reliability and safety of the systems themselves, reflecting the necessity for consistent and dependable operation of safety-critical systems. Additionally, emphasis is placed on fault tolerance, which pertains to the systems' ability to maintain functionality even in the presence of component failures. The verification of the implementation of the selected approaches is carried out through the justification and support of verification and validation processes.

D. Considered aspects of functional safety

The reviewed studies encompass both specialized tools and theoretical practices. Both approaches can be scaled to the level of practical implementation across the entire spectrum of the issues at hand. In this context, the question of specific implementation and the universalization of the approach is left to the end user. This creates an opportunity for growth in research related to defining the boundaries of applicability of individual methods for developing the limits of possible integration of these methods, aimed at alleviating some of the conservatism and constraints.

E. Key trends identified in the research

Current trends noted in the research include a shift towards the integration of modern modeling methods with traditional techniques. Concurrently, there is an increasing focus on software implementation processes, which encompasses enhanced verification and validation efforts, as well as approaches to justifying cybersecurity measures. Additionally, efforts are being made to optimize human-machine interfaces and to consider decision-making in dynamic environments. All of these initiatives aim to optimize the balance between safety, reliability, and the economic efficiency of existing solutions.

F. *Limitations of the presented research*

One of the significant aspects identified during the analysis is the lack of comparison between integrated approaches and the assessment of the level of conservatism in traditional methods. These factors may potentially serve as limitations to advancing research in the chosen subject area.

G.*Limitations of the study*

The analysis of the reviewed studies has identified a number of issues and limitations.

First and foremost, the challenges in the areas of modeling and data should be highlighted. Scalability issues hinder the application of formal methods to complex systems. Models, including operational ones, are often simplified to a binary representation of state ("functioning" / "not functioning"). There is a lack of operational data on emergency modes and data regarding the impact of degraded system conditions (e.g., component degradation) for conducting risk assessments based on PSA. This is characteristic of both

single-module and multi-module reactors. Collectively, this leads to concerns about the inadequacy of validation of existing failure data for use in specific operational contexts, types of equipment, and environmental conditions.

Additionally, modeling for the dispersion of external events should be considered. This class is also recognized as imperfect, with limitations in accounting for local meteorological conditions and impacts in atmospheric dispersion models. From the aforementioned issues arises a more global problem regarding the lack of experience with Level 3 PSA. This analysis is conducted less frequently than Level 1 and Level 2 PSAs, leading to a potential knowledge deficit in this area. Dependence on expert judgments and issues related to modeling failures within the software itself also represent ongoing limitations.

To compensate for these data limitations, conservative approaches are often employed, which can potentially lead to overestimation of risks and suboptimal decisions. The models used in analyses may overly simplify complex phenomena, failing to fully account for the influence of human factors, interactions between subsystems, and intricate physical processes. The associated resource constraints may result in an inability to model all possible accident scenarios, especially in systems susceptible to common cause failures for risk identification.

Further limitations arise when modeling complex dependencies within systems, particularly non-Markovian dependencies. Existing methods may also have constraints in accounting for temporal dependencies and the dynamic behavior of the system.

J.Prospects for research development

The conducted analysis allows for the identification of several promising directions for research in the area of growth within the chosen topic. Some of these directions are noted by the authors themselves.

One such improvement is the continued work on enhancing human-machine interfaces and the associated implementation of Human Reliability Analysis (HRA) methodologies. The results of these studies could be considered for creating a more complex integrated model that accounts for dynamic behavior, common cause failures, human factors, and cyber threats.

As previously mentioned, some of the implemented methodologies and methods are based on conservative approaches. In this context, research directions aimed at alleviating some of this conservatism appear promising. For example, the application of AI technologies in probabilistic analysis could partially address issues related to forecasting system behavior associated with aging.

The results of these studies can be linked to forecasting challenges. Further research directions lie in the development and refinement of dynamic reliability models, including non-homogeneous Markov processes, to tackle the "curse of dimensionality" in assessing the reliability of complex systems. This would allow for a more accurate consideration of the dynamic behavior of the system, including various states of component degradation. Addressing issues related to the impact of equipment aging, wear, environmental influences, and the possibility of hidden failures that are not detected during regular testing is also a critical area. Future research in this direction may focus on assessing the impact of "emergent" risks and factors that may arise from the interaction of individual subsystems, as well as the development of adaptive control systems capable of responding to changing operating conditions and equipment failures.

Conversely, the process of continuing research on hardware implementation can be highlighted. The development and application of analysis methods with fault injection at various levels of abstraction, from models to hardware implementation, offer a promising approach to studying the impact of failures on system behavior and evaluating the effectiveness of measures to prevent them

V. CONCLUSION

In this paper, we aim to identify gaps in the research on the risk-oriented approach to assessing the functional safety of reactor protection systems at NPPs. The study was conducted based on the analysis of 72 sources, during which metadata was extracted.

The analysis of the collected publications revealed a diversity of approaches and research directions covering aspects of the lifecycle, analysis, and optimization of instrumentation and control (I&C) systems. In the selected articles, the primary focus is on the scientific and practical justification of approaches to modeling and analyzing the reliability of modern digital I&C systems, the development and refinement of reliability models, quantitative assessment of various types of failures, and the application of automated tools for conducting verification and validation of solutions, which contributes to enhancing the reliability and safety of the systems.

Despite the existence of a comprehensive methodological framework and regulatory documents supporting the assessment of functional safety, significant areas for further development have been identified. In particular, there is a dependence on expert assessments, which may amplify subjectivity in the decision-making process. Furthermore, the application of a risk-oriented approach based on probabilistic models may lead to vulnerabilities in the selection of considered scenarios, which, in turn, could result in an incomplete risk assessment.

The results of this study underscore the need for further research in the area of assessing the functional safety of reactor protection systems, including the development of more comprehensive models that account for the dynamic behavior of systems and the interaction of subsystems. This will improve decision-making processes and enhance safety levels at nuclear power plants.

Our research helps to identify gaps in the current studies on the risk-oriented approach to assessing the functional safety of reactor protection systems and provides recommendations for researchers regarding topics related to PSA that are rarely addressed or could be considered promising directions for future research.

REFERENCES

[1] IAEA Safety Standards. Safety of Nuclear Power Plants: Design. Specific Safety Requirements. Series No. SSR-2/1 (Rev.1), 2016

[2] NP-001-15: Federal Rules and Regulations in the field of Atomic Energy Use. General Provisions for Nuclear Power Plant Safety

Assurance, Federal Service for Environmental, Technological and Nuclear Supervision, 2016. - 55p.
[3] IEC 61513: Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems = - Geneva: International Electrotechnical Commission, 2011. - 148 p.
[4] IAEA Safety standard. Safety of Nuclear Fuel Cycle Facilities. Specific Safety Requirements. Series No. SSR-4., 2017
[5] IEC 61508:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems. - Geneva : International Electrotechnical Commission, 2010.
[6] US NRC Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis. - Washington, DC : U.S. Nuclear Regulatory Commission, 2011
[7] NP-082-18 Requirements to the content and form of the safety analysis report for nuclear power plants (Requirements for Probabilistic Safety Analysis), The Federal Service for Environmental, Technological and Nuclear Supervision (Rostekhnadzor), 2018
[8] Morozov V.B. Improvement of models and methods for probabilistic safety analysis of NPP and their application in the design and operation on NPP with VVER reactors: 05.14.03 / Morozov V.B., Moscow, 2020
[9] Putilov A.V., Mokshin M. Yu. Predictive analysis of the sustainable development of a two-component nuclear power industry, Sustainable Innovative Development: Design and Management. 2023. Vol. 19, No. 2 (59). pp. 27-31, 2023
[10] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, “Systematic mapping studies in software engineering,” in 12th international conference on evaluation and assessment in software engineering, vol. 17, no. 1/sn, 01.06.2008, pp. 1–10, DOI:10.14236/ewic/EASE2008.8
[11] Ibrahim Ahmed, Enrico Zio, Gyunyoung Heo, Risk-informed approach to the safety improvement of the reactor protection system of the AGN-201K research reactor, Nuclear Engineering and Technology,Vo. 52, Is. 4, April 2020, pp. 764-775, DOI:10.1016/j.net.2019.09.015
[12] Y. Bulba, Y. Ponochovny, V. Sklyar, A. Ivasiuk Classification and Research of the Reactor Protection Instrumentation and Control System Functional Safety Markov Models in a Normal Operation Mode, ICTERI 2016, Kyiv, Ukraine, June 21-24, 2016, pp.308-321
[13] D. -A. Lee, J. Yoo and J. -S. Lee, Guidelines for the Use of Function Block Diagram in Reactor Protection Systems, 21st Asia-Pacific Software Engineering Conference, Jeju, Korea (South), 01.04.2014, pp. 135-142, DOI:10.1109/APSEC.2014.29
[14] Verrastro, Claudio & Estryk, D.S. & Rodriguez, G.F. & Ferrucci, Franco & Alarcón, J.E. & Ríos, G.E. & Lee, J.J.. FPGA Based Reactor Protection System Architecture, 16th IGORR 2014/IAEA Technical Meeting, November 2014
[15] Kazimierz T. Kosmowski Human Factors in Designing the Instrumentation and Control Systems Important to Safety, International Journal of Performability Engineering, 18.09.2014, Vol. 10, Iss. 7, pp.741-753
[16] Ma, Z., Yoshikawa, H., & Yang, M. Reliability model of the digital reactor protection system considering the repair time and common cause failure. Journal of Nuclear Science and Technology, 21.01.2017, 54(5), 539–551, DOI:10.1080/00223131.2017.1291375
[17] Muta, H., & Muramatsu, K. Quantitative modeling of digital reactor protection system using Markov state-transition model. Journal of Nuclear Science and Technology, 17.03.2024, 51(9), 1073–108, DOI:10.1080/00223131.2014.906331
[18] Sejin Jung, Junbeom Yoo, Young-Jun Lee, A PLC platform-independent structural analysis on FBD programs for digital reactor protection systems, Annals of Nuclear Energy, Vol. 103, May 2017, pp. 454-469, DOI:10.1016/j.anucene.2017.02.006
[19] Yichun Wu, Xuanxuan Shui, Yuanfeng Cai, Junyi Zhou, Zhiqiang Wu, Jianxiang Zheng, Development, verification and validation of an FPGA-based core heat removal protection system for a PWR, Nuclear Engineering and Design, Vol. 301, May 2016, pp. 311-319, DOI:10.1016/j.nucengdes.2016.03.018
[20] A. S. Saber, M. K. Shaat, A. El-Sayed, H. Torkey and M. A. Shouman, Reliability Analysis Model of the Digital Reactor Protection System, 37th National Radio Science Conference (NRSC), Cairo, Egypt, 26.10.2020, pp. 230-239, DOI:10.1109/NRSC49500.2020.9235117
[21] Liu, Kuanwei and Li, Zhaohua and Zhang, Binbin and Wang, Zhichao and Hu, Yuehua and Zhan, Wenhui and Yu, Zhangcheng, Research on the Impact of Maintenance Strategy for Protection and Safety Monitoring System on the Risk of Passive Nuclear Power Plants. 07.10.2024, SSRN: https://ssrn.com/abstract=4990157
[22] Ashutosh Kabra, Manoj Kumar, G. Karmakar, P. P. Marathe and A. P. Tiwari Dependability Analysis of Proposed I&C Architecture for Safety Systems of a Large PWR, Symposium on Advances in Control & Instrumentation (SACI-2014), 24-26.11.2014, Mumbai
[23] Marwa A. Shouman, Amany S. Saber, Mohamed K. Shaat, Ayman El-Sayed, Hanaa Torkey, A Hybrid Machine Learning Model for Reliability Evaluation of the Reactor Protection System, Alexandria Engineering Journal, Vol. 61, Iss. 9, September 2022, pp 6797-6809, DOI:10.1016/j.aej.2021.12.026
[24] Sejin Jung, Junbeom Yoo, Young-Jun Lee, A Software Fault Tree Analysis Technique for Formal Requirement Specifications of Nuclear Reactor Protection Systems, Reliability Engineering & System Safety, Vol. 203(3), June 2020, 107064, ISSN 0951-8320, DOI:10.1016/j.ress.2020.107064
[25] Kee-Choon Kwon, Jang-Soo Lee and Eunkyoung Jee A Framework for the Safety Assurance of Safety Software in Nuclear Power Plants, ISOFIC 2017, Gyeongju, Korea, 26-30.11..2017
[26] Torkey, H., Saber, A.S., Shaat, M.K. et al. Bayesian belief-based model for reliability improvement of the digital reactor protection system. Nuclear Science and Technologies 31(10), 11.10.2020, DOI:10.1007/s41365-020-00814-6
[27] Zhang, X., Yang, Hq., Yang, Jh., Deng, Xj. Forward Design of Nuclear Safety-Class DCS Based on Function Assignment and Signal New Energy Power Generation Automation and Intelligent Technology. SICPNPP 2024. Lecture Notes in Electrical Engineering, vol 1249. Springer, Singapore, 05.09.2024 DOI:10.3390/en17164063
[28] Zequn Lin, Lingzhi Wang, Yuanfeng Cai, Fanyu Wang, Yichun Wu, Implementation of a built-in self-test for nuclear power plant FPGA-based safety-critical control systems, Annals of Nuclear Energy, Vol. 165(1), January 2022, 108644, ISSN 0306-4549, DOI:10.1016/j.anucene.2021.108644
[29] Sejin Jung, Yoona Heo, Junbeom Yoo, A formal approach to support the identification of unsafe control actions of STPA for nuclear protection systems, Nuclear Engineering and Technology, Vol. 54(1), Iss. 5, October 2021, pp. 1635-1643, ISSN 1738-5733 DOI:10.1016/j.net.2021.10.033
[30] R. Khalil Ur and G. Heo, Risk Informed Design of I&C Architecture for Research Reactors IEEE Transactions on Nuclear Science, vol. 62(1), pp. 293-299, 29.01.2015 DOI:10.1109/TNS.2014.2375361 DOI:10.1109/TNS.2014.2375361
[31] K. U. Rahman, K. Jin and G. Heo, Risk-Informed Design of Hybrid I&C Architectures for Research Reactors, IEEE Transactions on Nuclear Science, vol. 63 (1), pp. 351-358, February 2016 DOI:10.1109/TNS.2015.2499779
[32] Steven A. Arndt, Rossnyev Alvarado, Bernard Dittman and Kenneth Mott NRC technical basis for evaluation of its position on protection against common cause failure in digital systems used in nuclear power plants 10th ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies At: San Fransico, CA, pp. 2031-2045 11-15.06.2017
[33] D Welbourne Safety critical software TN process control and nuclear power Icheme Symposium Series No. 141, 2016, pp.451-461
[34] Lee, Joonjae & Verrastro, Claudio & Estryk, D & Rossi, F & Quesada, G & Rodriguez, G & Ramos, N. Reliability Analysis for different configuration of a TRIP Final Actuator Interface for a Protection System of a Research Reactor, International Conference on Research Reactors: Addressing Challenges and Opportunities to Ensure Effectiveness and Sustainability Buenos Aires, Argentina, November 2019
[35] Q Z Liang, Y Guo and C H Peng A review on the research status of reliability analysis of the digital instrument and control system in NPPs, IOP Conference Series: Earth and Environmental Science, January 2020, 427(1):012018 DOI:10.1088/1755-1315/427/1/012018
[36] Chen, L.; Fan, D.; Zheng, J.; Xie, X. Functional Safety Analysis and Design of Sensors in Robot Joint Drive System. Machines 10(5), 360 18.04.2022, DOI:10.3390/machines10050360
[37] Ola Bäckström, Jan Erik Holmberg, Use of IEC 61508 in Nuclear Applications Regarding Software Reliabilit, 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability, Helsinki, June 2012

[38] N. Papakonstantinou and S. Sierla, Early phase fault propagation analysis of safety critical factory automation systems, IEEE 10th International Conference on Industrial Informatics, Beijing, China, June 2012, pp. 364-369, DOI:10.1109/INDIN.2012.6300856

[39] Qingzhu Liang, Yinghao Yang, Hang Zhang, Changhong Peng, Jianchao Lu,Analysis of simplification in Markov state-based models for reliability assessment of complex safety systems, Reliability Engineering & System Safety,Vol. 221, February 2022, 108373, ISSN 0951-8320, DOI:10.1016/j.ress.2022.108373

[40] Robert S Enzinnaa, Mariana Jockenhoevel-Barttfeldb, Yousef Abusharkhb, and Herve Bruneliere Modeling of Digital I&C and Software Common Cause Failures: Lessons Learned from PSAs of TELEPERM XS-Based Protection System Applications, PSAM 12, 2018

[41] Dong-Ah Lee, Junbeom Yoo, Jang-Soo Lee, A systematic verification of behavioral consistency between FBD design and ANSI-C implementation using HW-CBMC,Reliability Engineering & System Safety, Vol. 120 (3), pp. 139-149, December 2013, DOI:10.1016/j.ress.2013.06.006

[42] S. Li, J. Lou, X. Zong and S. Ma, Application of Fault Tree Analysis to the DCS Reliability of Nuclear Power Plants, IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 16-22.12.2022, pp. 1863-1868

[43] Masanobu Haruhara, Hitoshi Muta, Yasuki Ohtori, Shohei Yamagishi & Shota Terayama. Proposal of uncertainty analysis methodology for L1PRA using Markov state-transition model. Journal of Nuclear Science and Technology, 61(5), pp. 921-934, December 2023, DOI:10.1080/00223131.2023.2287111

[44] Liu, H, Liu, Z, Yang, X, Yan, S, & Chen, Z. The Safety Analysis of Multiple Method Fusion on Reactor Scram Subsystem Proceedings of the 2018 26th International Conference on Nuclear Engineering. Volume 6B: Thermal-Hydraulics and Safety Analyses. London, England. 22-26.07.2018, DOI:10.1115/ICONE26-82453

[45] Vyacheslav Kharchenko, Yuriy Ponochovnyi Artem Boyarchuk, Anton Andrashov Multi-Fragmental Markov Models of Information and Control Systems Safety Considering Elimination of Hardware-Software Faults, Proceedings of the 15th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops Kherson, Ukraine, 12-15.06.2019

[46] A.C. Torres-Echeverría, S. Martorell, H.A. Thompson, Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy, Reliability Engineering & System Safety, Vo. 94(2), pp. 162-179, February 2009 ISSN 0951-8320 DOI:10.1016/j.ress.2008.02.010

[47] Stefan Authen and Jan-Erik Holmberg Reliability analysis of digital systems in a probabilistic risk analysis for nuclear power plants, Nuclear Engineering and Technology, 44(5) pp.471-482 June 2012 DOI:10.5516/NET.03.2012.707

[48] S. Martorell, M. Villamizar, I. Martón, J.F. Villanueva, S. Carlos, A.I. Sánchez, Evaluation of risk impact of changes to surveillance requirements addressing model and parameter uncertainties, Reliability Engineering & System Safety, Vol. 126 (3), pp. 153-165, June 2014, ISSN 0951-8320 DOI:10.1016/j.ress.2014.02.003

[49] Tero Tyrväinen, Ola Bäckström, Jan-Erik Holmberg, Markus Porthin SICA – a software complexity analysis method for the failure probability estimation, Conference: 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), Seoul, October 2016

[50] Abiodun Ayodeji, Mokhtar Mohamed, Li Li, Antonio Di Buono, Iestyn Pierce, Hafiz Ahmed,Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors, Progress in Nuclear Energy, 161(9), 104738, May 2023, ISSN 0149-1970 DOI:10.1016/j.pnucene.2023.104738

[51] Pan, X.; Chen, H.; Shen, A.; Zhao, D.; Su, X. A Reliability Assessment Method for Complex Systems Based on Non-Homogeneous Markov Processes. Sensors, 24, 3446 May 2024, DOI:10.3390/s24113446

[52] Sejin Jung, Junbeom Yoo, Young-Jun Lee, A practical application of NUREG/CR-6430 software safety hazard analysis to FPGA software, Reliability Engineering & System Safety, 202(2), 107029, May 2020, ISSN 0951-8320 DOI:10.1016/j.ress.2020.107029

[53] Dong-Ah Lee, Eui-Sub Kim, Junbeom Yoo, Quantitative measures of thoroughness of FBD simulations for PLC-based digital I&C system, Nuclear Engineering and Technology, 53 (1), June 2020, pp. 131-141, ISSN 1738-5733 DOI:10.1016/j.net.2020.06.017

[54] Peter Bernard Ladkin Practical Statistical Evaluation of Critical Software, , University of Bielefeld and Causalis Limited Bev Littlewood, CSR, City University London, 01.03.2015

[55] Shi, GL., Wang, JW., Zhang, ZH., Zhang, ML., Li, L. (2022). Development and Application of Self-diagnosis and Analysis Function of FirmSys. Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems. ISNPP 2021. Lecture Notes in Electrical Engineering, 2022, vol 883. Springer 19.04.2022 https://doi.org/10.1007/978-981-19-1181-1_60

[56] Man Cheol Kim, Carol S. Smidts, Three suggestions on the definition of terms for the safety and reliability analysis of digital systems, Reliability Engineering & System Safety, Vol. 135, pp. 81-91, March 2015, ISSN 0951-8320 DOI:10.1016/j.ress.2014.10.022

[57] Jae-Cheon Jung, Hoon-Sun Chang and Hang-Bae KIM, "3+3 process" for safety critical software for I&C system in nuclear power plants, Nuclear engineering and technology, vol.41 No.1, February 2009

[58] Valkonen, Janne & Björkman, Kim & Holmberg, Jan-Erik & Lahtinen, Jussi & Pakonen, Antti & Tyrväinen, Tero & Heljanko, Keijo & Kuismin, Tuomas & Wieringa, Siert. Safety evaluation and reliability analysis of nuclear automation. Presentation of the SARANA project in SAFIR2014 Interim Seminar, 21-22.03.2013.

[59] Ola Bäckström, Jan-Erik Holmberg, Markus Porthin, Tero Tyrväinen Moding – modeling the reliability of digital I&C in modern nuclear power plants, 13th International Conference on Probabilistic Safety Assessment and Management, PSAM 13, October 2016

[60] A.C. Torres-Echeverría, S. Martorell, H.A. Thompson, Modelling and optimization of proof testing policies for safety instrumented systems, Reliability Engineering & System Safety, Vol. 94(4), pp. 838-854, April 2009, ISSN 0951-8320 DOI:10.1016/j.ress.2008.09.006

[61] Sejin Jung, Eui-Sub Kim, Junbeom Yoo, Jang-Yeol Kim, Jong Gyun Choi, An evaluation and acceptance of COTS software for FPGA-based controllers in NPPS, Annals of Nuclear Energy, Vol.94 (4), , pp 338-349, August 2016 ISSN 0306-4549 DOI:10.1016/j.anucene.2016.03.026

[62] Yuanfeng Cai, Yichun Wu, Junyi Zhou, Mingxing Liu, Qing Zhang, Quantitative software reliability assessment methodology based on Bayesian belief networks and statistical testing for safety-critical software, Annals of Nuclear Energy, Volume 145, 107593, September 2020, ISSN 0306-4549 DOI:10.1016/j.anucene.2020.107593

[63] J. Yoo, E. S. Kim, D. A. Lee, J. G. Choi, Y. J. Lee and J. S. Lee, "NuDE 2.0: A model-based software development environment for the PLC & FPGA based digital systems in nuclear power plants," 2014 International Symposium on Integrated Circuits (ISIC), Singapore, 10-12.12.2014, pp. 604-607 DOI:10.1109/ISICIR.2014.7029503

[64] Yiliu Liu, Safety barriers: Research advances and new thoughts on theory, engineering and management, Journal of Loss Prevention in the Process Industries, Volume 67(5), 104260, August 2020, ISSN 0950-4230 DOI:10.1016/j.jlp.2020.104260

[65] R.B.N. Vital, P.F. Frutuoso e Melo, J.A.C.C. Medeiros, M.A.B. Alvarenga, Availability assessment of a nuclear reactor limitation system by a Timed Petri Net, Progress in Nuclear Energy, Volume 152(5), 104380, October 2022, ISSN 0149-1970 DOI:10.1016/j.pnucene.2022.104380

[66] E.-S. Kim, D.-A. Lee, S. Jung, J. Yoo, J.-G. Choi, and J.-S. Lee, "NuDE 2.0: A Formal Method-based Software Development, Verification and Safety Analysis Environment for Digital I&Cs in NPPs," Journal of Computing Science and Engineering, vol. 11(1). pp. 9–23, 30.03.2017 DOI:10.5626/JCSE.2017.11.1.9

[67] Darpan Krishnakumar Shukla, A. John Arul, Static and dynamic reliability studies of a fast reactor shutdown system using smart component method, Annals of Nuclear Energy, Vol. 136(1), 107011 February 2020, ISSN 0306-4549 DOI:10.1016/j.anucene.2019.107011

[68] Kwang-Seop Son, Jae-Gu Song, Jung-Woon Lee, Development of the framework for quantitative cyber risk assessment in nuclear facilities, Nuclear Engineering and Technology, Vol.55(6), March 2023, pp. 2034-2046, ISSN 1738-5733 DOI:10.1016/j.net.2023.03.023

[69] W. Ma, B. Wen, B. Xu, H. Yan and L. Zhou, Optimization of Reliability in ACP100 Automatic Depressurization System Squib Valve Control System," 2024 Global Reliability and Prognostics and

Health Management Conference (PHM-Beijing), Beijing, China, 11-13.10.2024, pp. 1-6, doi: 10.1109/PHM-Beijing63284.

[70] Mariana Jockenhövel-Barttfelda Stefan Karga, Christian Hesslerb and Herve Bruneliere, Reliability Analyses of Digital I&C Systems within the Verification and Validation Process, Probabilistic Safety Assessment and Management PSAM 14, 2018, Los Angeles, CA,

[71] Kharchenko, V., Ponochovnyi, Y., Boyarchuk, A., Andrashov, A., Rudenko, I. Multi-fragmental Markov's Models for Safety Assessment of NPP I&C System Considering Migration of Hidden Failures. Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2019. Communications in Computer and Information Science, vol 1175., pp.302-326 January 2020, Springer, Cham DOI:10.1007/978-3-030-39459-2_14

[72] Wu, ZG., Zhu, J., Yu, XB. Reliability Analysis of Tripping Solenoid Valve Power System Based on Dynamic Fault Tree and Sequential Monte Carlo. Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems. ISNPP 2021. Lecture Notes in Electrical Engineering, vol 883. April 2022, pp.148-158, Springer, Singapore DOI:10.1007/978-981-19-1181-1_14

[73] Haruhara, M., Muta, H., Ohtori, Y., Yamagishi, S., & Terayama, S. Proposal of uncertainty analysis methodology for L1PRA using Markov state-transition model. Journal of Nuclear Science and Technology, 61(5), pp.921–934. December 2023 DOI:10.1080/00223131.2023.2287111

[74] Junbeom Yoo, Eui-Sub Kim2, Dong Ah Lee3, and Jong-Gyun Choi An Integrated Software Development Framework for PLC & FPGA based Digital I&Cs, ISOFIC/ISSNP 2014, Jeju, Korea, 24-28.08.2014

[75] Phillip McNelles, Zhao Chang Zeng, Guna Renganathan, Greg Lamarre, Yolande Akl, Lixuan Lu, A comparison of Fault Trees and the Dynamic Flowgraph Methodology for the analysis of FPGA-based safety systems Part 1: Reactor trip logic loop reliability analysis, Reliability Engineering & System Safety, Vol. 153(5), May 2016, pp. 135-150, ISSN 0951-8320 DOI:10.1016/j.ress.2016.04.014

[76] E. Nouri, N. Nosrati, H. T. Asl, M. R. Manavand and Z. Navabi, "Multi-Level Fault Injection Methodology Using UVM-SystemC," 2023 IEEE East-West Design & Test Symposium (EWDTS), Batumi, Georgia, September 2023, pp. 1-6 DOI:10.1109/EWDTS59469.2023.10297034

[77] Xi, CH., Sun, W., Zhang, LM. The Software Modeling and Sensitivity Study of Computer Based I&C System in Probabilistic Safety Assessment of Nuclear Power Plant. Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems. ISNPP 2021. Lecture Notes in Electrical Engineering, vol 883. pp.97-103 19.04.2022, ,Springer, Singapore DOI: 10.1007/978-981-19-1181-1_10

[78] Lin, YJ., Yang, JM., Wang, RY., Yang, YX. Research on Common Cause Fault Evaluation Model of RTS Based on β-factor Method. Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems. ISNPP 2021. Lecture Notes in Electrical Engineering, vol 883. pp.590-599, Springer, Singapore 19.04.2022, DOI:10.1007/978-981-19-1181-1_57

[79] Athira Varma Jayakumar, Systematic Model-based Design Assurance and Property-based Fault Injection for Safety Critical Digital, Virginia Commonwealth University, Richmond, Virginia, 2020

[80] H. Tu, L. Yao, X. W. Zhai, C. Gui and X. Fan, Reliability Test Method of Nuclear Power DCS Network Communication Based on Fault Injection," 2023 8th International Conference on Computer and Communication Systems (ICCCS), Guangzhou, China, 21-23.04.2023 doi: 10.1109/ICCCS57501.2023.10150497.

[81] Y. Nakata et al., "Model-based fault injection for failure effect analysis — Evaluation of dependable SRAM for vehicle control units," IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), Hong Kong, China, June 2011 DOI:10.1109/DSNW.2011.5958842

[82] Yasuo Sugure, Yasuhiro Ito, Yohei Nakata, Yusuke Takeuchi, Hiroshi Kawaguchi, Masahiko Yoshimoto, Shigeru Oho, Failure Modes and Effects Analysis Using Virtual Prototyping System with Microcontroller Model for Automotive Control System, IFAC Proceedings Volumes, Advances in Automotive Control Volume 46(21), September 2013, pp. 562-563, ISSN 1474-6670, ISBN 9783902823489 DOI:10.3182/20130904-4-JP-2042.00103

[83] PLCopen TC6. Guidelines for the use of PLCs in safety-related applications. PLCopen, 2015

[84] IEC 60880. Software for computers in the safety systems of nuclear power plants. International Electrotechnical Commission, 2013.

[85] ERPI NP-5652/TR-1025243. Guidelines for the use of software in safety-related systems. ERPI, 2010.

[86] SanPiN 2.6.1.2523-09. Radiation Safety Standards (NRB-99/2009). Approved by the decree of the Chief State Sanitary Doctor of the Russian Federation dated December 30, 2009, No. 58