IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 8 August 2023, accepted 27 August 2023, date of publication 30 August 2023, date of current version 6 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3310249

RESEARCH ARTICLE

A Predictive Dynamic Approach to Evaluating the Reliability of Passive Systems

AKMALI MASOOD AND PLANA ROBERT, (Senior Member, IEEE)
Assystem Energy and Operation, 92400 Courbevoie, France
Corresponding author: Akmali Masood (makmali@assystem.com)

ABSTRACT Passive systems play a vital role in ensuring the safety and advancement of Nuclear Power Plant (NPP) technology. The precise evaluation of their reliability is of paramount importance for their successful implementation in the nuclear industry. A thorough understanding of the reliability of these passive systems is essential to ensure the safety and efficiency of nuclear power plants, making them a cornerstone of nuclear energy generation. A new methodology has been developed to assess the reliability of passive systems, which are distinguished by three main components: systematic functional analysis, dynamic component analysis, and phenomenological factors. Each step of the methodology is described and commented, and a diagram of the methodology is presented. The paper presents a novel approach for analysing dynamic systems by incorporating dependencies among events and component states, as well as accounting for the impact of phenomenological factors. A state space solution to generate all possible system states and stochastic transitions is proposed, resulting in a Continuous Time Markov Chain (CTMC) representation of the system's behaviour. To support this analysis, an algorithm that integrates multiple phenomenological factors by sampling their values from respective probability distributions is also developed. Through Monte Carlo simulation, the approach provides a comprehensive and realistic assessment of the system's performance, enabling accurate reliability analysis and decision-making.

INDEX TERMS Passive system reliability. probabilistic safety assessment, model based safety assessment, generalized stochastic Petri net.

I. INTRODUCTION

Reliability R(t) [1] is a commonly used measure to quantify the dependability of safety or mission-critical systems. It represents the probability that a system performs its required function within the time interval (0, t). To evaluate the reliability or unreliability of a system, constructing models is a common approach. These models can be based on various techniques such as fault trees, stochastic Petri nets, or Markov chains [1]. By constructing and analysing these models, it becomes possible to estimate the reliability or unreliability of the system, as well as other dependability measures of interest. These models provide insights into the system's behaviour, failure modes, and factors influencing its performance, facilitating decision-making processes related to system design, maintenance strategies, and risk mitigation [2].

To analyse a dynamic system that is dependent on physical phenomenon factors, one would need to identify the relevant physical variables and their relationships. Nuclear passive safety systems can be among those dynamic systems that depend on physical phenomenon factors. These systems are designed to use physical processes such as natural convection, gravity, or phase change to safely shut down a nuclear reactor and prevent the release of radioactive materials in the event of an accident or loss of power [2], [3], [4]. The behaviour of these systems is influenced by physical variables such as temperature, pressure, and flow rates, and their performance is subject to uncertainties and variability. Therefore, analysing and assessing the reliability of nuclear passive safety systems requires a thorough understanding of the physical phenomena involved. This may involve using mathematical models, simulations, or experimental data to understand the behaviour

The associate editor coordinating the review of this manuscript and approving it for publication was Sajid Ali.

of the system over time. Additionally, it is important to consider the uncertainties and potential sources of variability that may impact the system's performance or reliability. The dependability of passive safety systems is a contemporary issue that confronts today's advanced reactors, especially Small Modular Reactors (SMR). It is also a relatively new area that is driven by technological advancements and safety regulations.

Despite recent developments [5], [6], [7], [8], there remain technological challenges and issues in incorporating passive systems into reactor designs. One key challenge is accurately quantifying the functional reliability of these systems during normal operation, transients, and accidental conditions. Functional failures in passive systems can occur due to deviations in boundary conditions or geometric parameters, as the driving forces in passive systems are relatively small and can be affected by small changes in operating parameters or system geometry [2], [3], [4]. The reliability and availability of a passive system depend primarily on two factors: the integrity and functionality of its components and the confidence with which it can perform under all required conditions, such as thermal-hydraulic performance.

Recent research in reliability has introduced new evaluation methodologies for engineering systems that aim to improve the understanding of system performance and resilience. One such approach is the use of dynamic-Bayesian-network-based degradation and maintenance, which can provide more accurate predictions of the behaviour of engineering systems over time [6]. Another approach is the development of availability-based engineering resilience metrics, which provide a new measure of system resilience and can be used to inform decision-making. The use of Bayesian networks in reliability evaluations has also been explored, enabling the incorporation of uncertainties and dependencies into the analysis of engineering systems [7].

Researchers have explored the use of both static and dynamic fault trees for system analysis. Static fault trees are typically used to model the failure events and their dependencies that can lead to system failure. In contrast, dynamic fault trees can capture the time-dependent behaviour of a system and account for the impact of repairs, maintenance, and other factors on system performance.

One approach that has been proposed is to combine static and dynamic fault trees to provide a more comprehensive analysis of system reliability. For example, a study by Baek, Sejin et al. [7] proposed a hybrid fault tree model that integrates partially static and dynamic fault trees to analyse the reliability of certain systems. The model used static fault trees to identify the failure events and their dependencies, while dynamic fault trees were used to capture the time-dependent behaviour of the system and the impact of repairs and maintenance on system performance.

Another study by Khare, Vikas et al. [7] proposed a similar approach, where a hybrid static-dynamic fault tree model was used to analyse the reliability of a hybrid renewable power station. The model used static fault trees to identify the failure events and their dependencies, while dynamic fault trees were used to capture the time-dependent behaviour of the system and the impact of repairs and maintenance on system performance.

Overall, the use of a hybrid static-dynamic fault tree model can provide a more comprehensive analysis of system reliability by accounting for both the static and dynamic aspects of the system. This approach can lead to improved decision-making regarding the design, operation, and maintenance of engineering systems.

These evaluation methodologies integrate both static and dynamic aspects of the system to provide a more comprehensive understanding of system performance and reliability. They can inform the design, operation, and maintenance of engineering systems, improving their safety and reliability. Overall, the development and application of these evaluation methodologies are essential for the continued improvement of engineering systems and their resilience to unforeseen events.

The use of qualitative and quantitative methodologies in reliability and risk assessment studies contributes to increased safety and reliability. In the past, various methodologies such as Methodology for the Reliability Assessment of Passive System ReliAbility (APSRA) [9] and Methods for Passive Safety Functions (RMPS) [10] have been developed to evaluate the reliability of passive systems. However, when implementing the RMPS or mechanistic method for assessing the reliability of passive systems and integrating it with plant-specific probabilistic safety assessment (PSA), certain shortcomings become apparent. These issues can be summarized as follows:

1) The methodology used in mechanistic approach such as RMPS [8] does not take into account the interaction between hardware/component failure and the functional failure of passive systems. It is possible that hardware/component degradation during the operation of passive systems may result in functional failure. This fault tree treatment of considering the hardware failure and functional failure of passive systems separately could be improved.

2) The event tree treatment of passive systems is only applicable to one accident scenario, and each passive system needs to be analysed separately for different initiating events and accident scenarios. This could result in a computationally intensive scheme.

3) Instead of using classical PSA treatment based on the assumptions of the same failure rates of components throughout the mission time, a more advanced form of PSA such as dynamic probabilistic safety assessment (DPSA) [8] can be utilized for implementing risk-informed decision making.

4) Best estimate codes based on phenomenological simulations of natural convection passive systems may have significant uncertainties that need to be incorporated appropriately in the performance and reliability analysis of such systems.

5) The REPAS, RMPS, and APSRA [7], [8], [9] methodologies do not consider dynamic failures of components or processes that could strongly influence the failure of passive systems. To address this, a dynamic reliability methodology based on Monte Carlo simulation can be used to present the influence of dynamic failure characteristics of components on system failure probability.

As severe accidents are being considered more extensively and safety requirements are increasing, there is a growing interest in passive safety systems for future nuclear reactors. These systems are effective and transparent and are often used in combination with active safety or operational systems in innovative reactor concepts. Passive systems, as defined by the IAEA (1991) [2], do not require external energy to operate and offer benefits such as simplicity, decreased need for human interaction, and reduced dependence on external electrical power or signals. However, there are challenges to consider, including a lack of data on certain phenomena and a smaller range of driving forces compared to active safety systems. Additionally, economic competitiveness remains an important factor to consider.

The purpose and motivation behind developing this new dynamic methodology for reliability evaluation of safety systems, particularly passive systems, lies in the need for improved safety measures and risk assessment in nuclear power plants. The existing methodologies, such as RMPS, APSRA, and REPAS, have shown limitations in adequately addressing the dynamic behaviour and interactions within passive systems. The proposed methodology bridges these gaps and presents a more comprehensive and accurate assessment, enabling better-informed decision making for the nuclear industry. By incorporating dynamic component analysis, systematic functional analysis, and accounting for phenomenological factors, the new method provides a more realistic representation of system behaviour and failure modes. It allows for a more advanced form of probabilistic safety assessment (DPSA), accommodating uncertainties in best estimate codes and addressing the influence of dynamic failures of components. With the integration of Monte Carlo simulation, the methodology offers a powerful tool for capturing complex system dynamics and optimizing safety strategies. Overall, the development of this new dynamic reliability evaluation methodology aims to enhance the safety, reliability, and risk management of nuclear power plants, ensuring safer and more efficient operation in the nuclear industry.

A specific methodology was deemed necessary to evaluate the reliability of passive system B or C (i.e. implementing moving working fluid, following the IAEA (1991) classification). This methodology is developed within the R&D activities carried out by Innovation department of Assystem[1]. The methodology focuses on predictive dynamic reliability assessment through functional analysis of the system and its components, as well as the integration of phenomenological factors.

II. METHODOLOGY OVERVIEW

The proposed dynamic methodology for evaluating the reliability of safety systems, including passive systems, represents a significant innovation in the field of nuclear safety and risk assessment. Unlike traditional methodologies, the new approach integrates three main components: systematic functional analysis, dynamic component analysis, and consideration of phenomenological factors. By combining these elements, the methodology offers a comprehensive and realistic assessment of the reliability of passive systems, taking into account the dynamic nature of their behaviour and the influence of various external factors. This dynamic methodology addresses the shortcomings of previous approaches, such as the lack of interaction consideration between hardware/component failure and functional failure of passive systems, the need for separate analyses for each passive system and initiating events, and the inability to capture dynamic failures of components or processes. With the incorporation of Monte Carlo simulation, the influence of dynamic failure characteristics of components on system failure probability can now be presented. The new methodology provides a more advanced form of probabilistic safety assessment (DPSA) and enables risk-informed decision making, contributing to increased safety and reliability in nuclear power plant technology.

The proposed methodology consists of several elements, which are illustrated in Fig. 1 and described in more detail in the following sections.

III. THE MAIN ELEMENTS

The proposed methodology is based on integration of dynamic components analysis into static functional analysis of the system, incorporation of phenomenological analysis.

Systematic functional analysis, including methods like Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) [9], helps identify the potential failure modes and their consequences in a structured manner. These methods analyse the system from a top-down perspective and identify the critical paths and components that may cause the system to fail. Systematic functional analysis also helps identify the measures to prevent or mitigate the effects of failures. Component dynamic analysis, including methods like Dynamic Fault Tree (DFT) [9], [10], [11], [12] analysis, takes into account the dynamic behaviour of the system components and their interactions with each other over time. This analysis can help evaluate the reliability of individual components and how their performance affects the overall system reliability. Component analysis can also help identify the potential failure modes of the individual components and their consequences.

Phenomenological factors, such as environmental and operational conditions, can significantly affect the performance and reliability of a passive safety system [2], [3]. These factors are often difficult to predict or model accurately, but their impact on the system reliability should not be ignored. Including phenomenological factors in the reliability

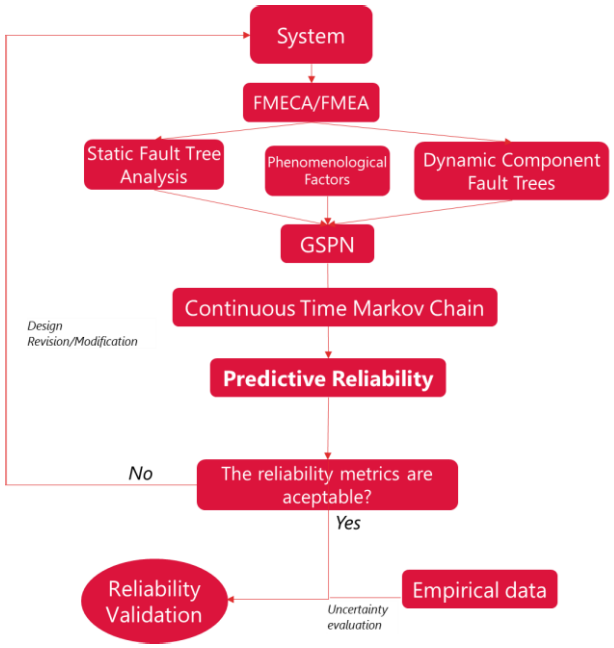

FIGURE 1. Commonly used logic gates in DFT.

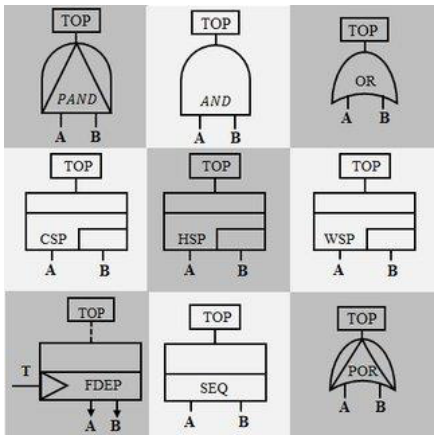

FIGURE 2. The proposed methodology for safety system (passive).

evaluation helps assess the system's behaviour under different operating conditions and how these conditions affect the system's reliability.

To understand why it is necessary to consider both static and dynamic aspects of a system and incorporate the physical phenomena factors, let's take the example of a nuclear reactor.

The static aspect of a nuclear reactor involves its design, materials, and geometry. These factors affect the behaviour of the system under normal operating conditions and provide the basis for safety analysis. For instance, the containment structure and fuel cladding are designed to withstand high temperatures and pressures and prevent the release of radioactive materials.

However, the dynamic behaviour of a nuclear reactor is also crucial to its safety. This includes the response of the system to changes in operating conditions or the occurrence of abnormal events, such as a loss of coolant accident. Physical phenomena such as heat transfer, fluid mechanics, and thermodynamics play a critical role in determining the behaviour of the system under these conditions.

Therefore, to study the safety of a nuclear reactor, it is necessary to consider both the static and dynamic aspects of the system and integrate physical phenomena factors.

The following formula is used to prioritise failure modes based on their risk priority number, which is a quantitative measure of the potential risk associated with a specific failure mode [11]. In FMEA, the Risk Priority Number (RPN) is calculated as the product of three values:

$$RPN = S \times O \times D \tag{1}$$

where:

S is the Severity rating (typically on a scale of 1-10),

O is the Occurrence rating (typically on a scale of 1-10), and

D is the Detection rating (typically on a scale of 1-10).

Dynamic Component Analysis: This type of analysis focuses on the individual components of the system and how their performance affects the overall system reliability. Dynamic Fault Trees (DFTs) [14], [15], [16], [17], [18], [19] are a common technique used in component analysis. Figure 2 shows graphical symbols of the commonly used DFT gates. The DFT can: (1) management of spare components and their allocation, (2) the functional dependency, and (3) the failure sequence dependency. They allow us to model the interactions between different components of the system over time and calculate the probability of different failure scenarios. By simulating the behaviour of the system over time, we can evaluate its reliability and identify potential failure modes. The probability of a top event in a Dynamic Fault Tree (DFT) can be calculated using the following equation [13]:

$$\mathrm{P}\left(TopEvent\right) = 1 - \prod_{i=1}^{n} \left(1 - Gate_i\right)^{-1} \tag{2}$$

where $\mathrm{P}(Gate_i)$ is the probability of the i^{th} gate in the DFT being successful (i.e. not failing).

The probability of a component failure in a DFT can be calculated using the following equation:

$$P\left(ComponentFailure\right) = \sum_{j=1}^{m} P\left(FailureMode_j\right) \times P(Mode_j \rightarrow Component)) \tag{3}$$

where $P\left(FailureMode_j\right)$ is the probability of failure mode j occurring, and $P\left(Mode_j \rightarrow Component\right)$ is the probability that failure mode j will cause a failure of the component.

Integrating dynamic fault tree analysis into static fault tree analysis offers several advantages, including the management of spare components and their allocation, consideration of functional dependency, and analysis of failure sequence dependency:

A. MANAGEMENT OF SPARE COMPONENTS AND ALLOCATION

Integrating dynamic fault tree analysis allows for the consideration of spare components and their allocation strategies. By modeling the availability and repair processes of spare components, the analysis can provide insights into the optimal allocation of spare components within the system. This helps in managing inventory, reducing downtime, and ensuring the system's availability during failures.

B. FUNCTIONAL DEPENDENCY

In many systems, the failure of one component can affect the functioning of other components. By integrating dynamic fault tree analysis, functional dependency between components can be captured. This means that the occurrence or failure of one event in the fault tree can dynamically propagate to other events, considering the dependencies and their impact on the system's reliability. It enables a more accurate assessment of the system's behaviour and potential failure scenarios.

C. FAILURE SEQUENCE DEPENDENCY

Failure sequence dependency refers to the order in which failures occur within the system and their impact on subsequent events. Dynamic fault tree analysis considers the temporal aspect of failures and incorporates failure sequence dependencies. It allows for modeling the cascading effects of failures, where the occurrence of one failure event can trigger or inhibit other events in the fault tree. By capturing the failure sequence dependencies, the analysis can provide insights into the system's behaviour over time and the potential consequences of failure events.

By integrating phenomenological factors, such as human errors, environmental conditions, and operational factors, into the fault tree analysis, the model can evaluate the predictive reliability of the dynamic system. This enables the assessment of the system's performance under various operational conditions and the identification of potential vulnerabilities and improvement opportunities and aids in making informed decisions regarding system design, maintenance strategies, and risk mitigation measures.

The overall risk associated with a system can be calculated using the following equation [18]:

$$Risk = \sum \left(P\left(Failure_i\right) \times Consequence_i \right) \qquad (4)$$

where $P\left(Failure_i\right)$ is the probability of failure scenario i occurring, and $Consequence_i$ is the consequence (in terms of human or environmental impact) of failure scenario i.

The probability of an external event (e.g. earthquake, operator error) can be estimated using historical data, expert judgment, or other sources of information. For example, the probability of an earthquake occurring in a given region in a given year can be estimated using statistical models based on historical earthquake data.

The Fault Tree (FT) is a widely used stochastic model for analysing the unreliability of complex systems. It represents how combinations of component failure events can lead to the failure of subsystems or the entire system using Boolean gates. In the standard version of FT, component failure events are assumed to be statistically independent, which simplifies the computation of system unreliability but limits the modeling capabilities. Dynamic Fault Tree (DFT) is an evolution of FT that addresses the limitation of assuming independence among events or component states. DFT introduces dependencies among events and component states, requiring a state space solution to generate all possible system states and stochastic transitions between them. This involves obtaining the Continuous Time Markov Chain (CTMC) [18] of the system.

In real systems, the separation of independent and dependent failures can be extended to smaller granularities by modeling each set of reused components with its respective fail rate. This not only allows for a more accurate model but also allows sets of reused components to span over subsets of systems.

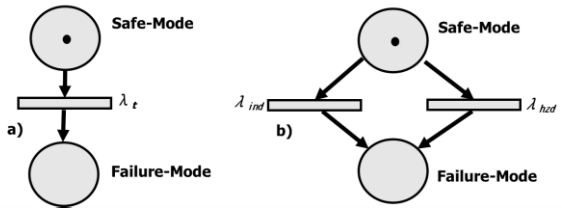

FIGURE 3. Simple generalised stochastic Petri nets, (a) Single-mode Model, (b) Multi-mode model [20].

IV. PETRI NETS ANALYSIS

Petri nets [20] can be a helpful tool in analysing the three factors of fault tree analysis, and dynamic fault tree analysis for components and phenomenological factors in order to evaluate reliability estimation for a passive safety.

The generalised stochastic Petri net (GSPN) is a Petri net extension where each transition (timed /immediate) is linked to an exponentially distributed random variable expressing the delay [9], [10].

The transition from DFT to GSPN enables the state space solution by generating the CTMC, facilitating the computation of system unreliability. The definition of GSPN primitives has been expanded to include their usefulness in modeling common-mode faults and cascading effects. Figure 3 shows the simplest GSPN primitive for a simple system, with safe-mode and failure-mode places representing the state of the infrastructure. The fail rate of λ_t applies in a single-mode fault model. Petri nets can be used to determine the reliability of a system, where R(t) is defined as the probability of the system functioning throughout the entire time interval [0, t], given that it was functioning at t=0. Introducing common mode failure models partitions the fail rates, resulting in rates for faults obeying the independence of those who assume faults and those who do not.

Partitioning the fail rate in the simple model of Fig. 3.a results in the GSPN primitive shown in Fig. 3.b. The aggregate fail rate is given by the sum of the fail rates for independent and common mode faults. The multi-mode GSPN primitive can be used to derive a common-mode failure GSPN primitive for a two-system scenario, as shown in Fig. 3.b. The common mode fault affecting both systems is modeled by the subnet in the centre, consisting of place com and its associated timed transition with a fail rate of λ_{hzd}. Each system may fail independently as a result of the firing of their timed transition with rate λ_{ind}, but both systems fail if the center transition fires. The fail rate of the center transition does not depend on the markings of places Sys-i-up and Sys-j-up because it represents the common mode failure of two systems subjected to the same input.

Efficient techniques for generating the CTMC from a Generalized Stochastic Petri Net (GSPN) are available in tools like GreatSPN [1], [18]. Therefore, to perform the state space solution of a DFT, the DFT can be converted into an equivalent GSPN. From the GSPN, the CTMC can be generated, allowing for the computation of the system's unreliability based on the CTMC.

Fig. 4 shows the PN models of the Boolean and dynamic gates used in DFTs. As seen in the PN model of the AND gate in Fig. 4(a), all input places: In Figure 4, the PN models of the Boolean and dynamic gates used in DFTs are displayed. The PN model of the AND gate in Figure 4(a) shows that all input places, X_1:dn to X_n:dn, are connected to a single immediate transition called AND. When all input places receive a token, the transition AND will activate, causing the AND gate output to become true by depositing a token to the place X.dn. On the other hand, the PN model of the OR gate in Figure 4(a) represents a disjunctive behaviour.

Each input place, X_i:dn, is connected to a distinct immediate transition, ensuring that when any of the input places receive a token, the corresponding transition will activate, making the OR gate output true by depositing a token to the place X.dn. Figure 4(c) shows the PN model of the PAND gate, which is designed to ensure that the place (X.dn) representing the output of the PAND gate receives a token only when the input places receive tokens in a sequential order, according to the required sequencing of the basic events (BEs). If the order of occurrence of the BEs is disrupted, the place X.ok will receive a token, preventing the transition T_n from firing and forcing the PAND output to be false.

To incorporate the three mainly used probability distributions (exponential distribution, normal distribution, Poisson distribution) [20] into the Petri net analysis, a stochastic Petri net model is typically augmented with additional information, such as transition rates or probabilities, and then analysed using stochastic simulation techniques. The simulation generates a large number of sample paths, each representing a possible sequence of events and transitions, and calculates the likelihood of various outcomes based on these sample paths.

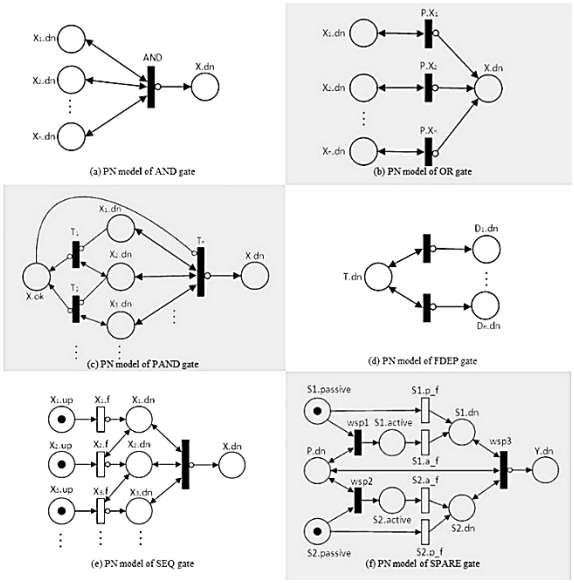

FIGURE 4. PN models of Boolean and dynamic gates.

Once the PN model is created, it can undergo various forms of evaluation to perform different types of analyses. For instance, if all the timed transitions in the PN model follow an exponential distribution, then the underlying Markov model can be used for evaluation. However, this analysis is limited to only exponentially distributed failure data. In contrast, if the PN model contains non-exponentially distributed timed transitions, then Monte Carlo simulation can be used, but this approach is computationally time-consuming [18]. While PNs allow for more flexibility in using different types of distributions, they share many features with Markov models. Both PN-based and Markov model-based approaches require generating the state space of the system for analysis, which leads to the state space explosion problem when dealing with moderately complex systems. In the seminal work of Bobbio et al. [22], it was demonstrated how a classical static fault tree could be evaluated by translating it to Petri Nets (PN). This approach has inspired the use of PN in different methods for evaluating DFTs.

Once the probabilities are assigned to the places and transitions in the SPN model, the reliability of the passive safety system can be evaluated by simulating the model over a large number of iterations. This can be done using Markov chain Monte Carlo simulation. During the simulation, the model generates a set of possible system states and their associated probabilities. By analysing the results of the simulation, the most probable failure modes and the potential consequences of failure for the system can be identified. This information can be used to optimize the design of the system and to develop strategies for minimizing the risk of failure.

Figure 5 illustrates a visual representation of how SPN and uncertain external influencing phenomenological factors can be integrated. The transition rates in this model are influenced

by a vector of n random parameters with a joint probability distribution.

The values of these parameters impact the transition rates and, therefore, the overall behaviour of the system. Equation (5) describes the general form of the transition rate, and the total rate of departure from state i can be calculated based on this equation:

$$\lambda(t,\theta) = \sum_{i=0, j\neq i}^{m} \lambda_{ij}(t,\theta) \tag{5}$$

To incorporate external influencing phenomenological factors, the following steps should be followed:

1) Formulate the functions that describe the physical relationship between the system and the transition rates.
2) Identify the specific external influencing factors that can impact the system's behaviour, such as pressure, temperature, vibration, or stress.
3) Define the distribution functions $P(\theta)$ that represent the uncertainties associated with these external influencing factors θ_i. These distribution functions help capture the variability or unpredictability in the values of these factors, allowing for a more comprehensive analysis of the system's performance under different conditions.

V. MONTE CARLO SIMULATION

In Monte Carlo (MC) simulation, the probability distribution function $P(\theta)$ is not directly sampled [20]. Instead, the simulation involves sampling the holding time at each state and determining the transition from the current state to another state. This process is repeated iteratively until the accumulated holding time reaches the predefined time horizon.

To calculate the transition probability, the following steps are followed:

1) Begin at the initial state i.
2) Sample the holding time at the current state i. This is done by generating a random value from the distribution function that represents the holding time at state i.
3) Determine the next state j by evaluating the transition probabilities from state i to all possible states. This is done by comparing the sampled holding time to the cumulative probabilities of the transitions. The next state j is selected based on the interval in which the sampled holding time falls.
4) Move the system to the next state j.
5) Repeat steps 2-4 until the accumulated holding time reaches the predefined time horizon or the system reaches an absorbing state.

By performing this iterative process, a time sequence is generated that consists of the holding times at different states. This time sequence provides information on the duration of the system's stay at each state during the simulation. The transition probabilities are implicitly accounted for through the sampling of holding times and the subsequent state transitions.

This Monte Carlo simulation approach allows for the estimation of the transition probabilities in an Implicit Continuous-Time Markov Chain (ICTMC) model. It provides a probabilistic representation of the system's behaviour over time, taking into account the uncertainties associated with the holding times and the stochastic nature of the transitions between states.

A generalized version of the algorithm that simulates the incorporation of any phenomenological factors in a nominal transition process (failure modes):

1. Initialize the system by placing a token in the initial state $i = M$ (representing perfect performance).
2. Set the initial time $t = 0$ and define the maximum number of replications as N_{max}.
3. Set $t' = 0$ and initialise the replication counter $n = 1$.
4. While $n < N_{max}$:
   a. Set $t = 0$.
   b. While $t < t_{max}$:
      i. Sample realisations of the phenomenological factors (external influencing factors) from their respective probability functions.
      ii. For each phenomenological factor:
      - Sample a value for the factor from its probability distribution.
      iii. Sample a departure time t from the distribution function $F_i(t \mid t', \theta)$ considering the values of the phenomenological factors.
      iv. Sample a random number U from the uniform distribution in the range [0, 1].
      v. For each outgoing transition ($j = 0, 1, \ldots, M, j \neq i$):
      - Calculate the transition probability $q_{i,j}(t \mid \theta$, factor values).
      - If $\left(\sum_{k=0}^{j^*-1} q_{i,k} < U < \sum_{k=0}^{j^*} q_{i,k}\right)$ activate the transition to state j^*.
      vi. Set $t' = t$.
      vii. Remove the token from state i and place it in state j^*.
      viii. Increment t by the sampled departure time t.
   c. Increment n by 1.
5. Compute the state probability vector by dividing the total number of visits to each state by the total number of simulations.

In this algorithm incorporates multiple phenomenological factors (F) by sampling their values from their respective probability distributions $P(\theta)$. These factors can represent various external influences on the component failure modes, such as pressure, temperature, vibration, stress, humidity, etc. The sampled factor values are then considered when sampling the departure time and calculating the transition probabilities. This allows for a more realistic simulation that accounts for the uncertainties and variability introduced by the phenomenological factors in the failure modes. The state probability vector represents the probability distribution of the system being in each state after running the simulations. It is computed by counting the total number of visits to each

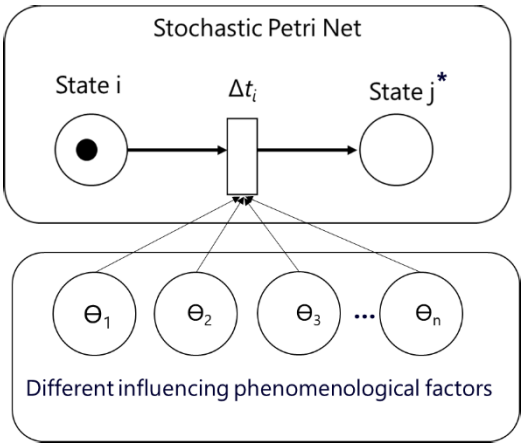

FIGURE 5. Graphical illustration of the integrated model.

state across all replications and dividing it by the total number of simulations.

The algorithm takes into account the phenomenological factors, which are sampled from their respective probability functions, to simulate the degradation process of the component. The use of the algorithm allows for the estimation of the probabilities associated with each state, providing valuable insights into the system's performance and reliability.

Further work is planned to apply the proposed approach into GSPN to evaluating the reliability of passive safety system incorporating the elements before being incorporated into Model-based Safety Analysis (MBSA) [21], [22] to provide a more accurate and comprehensive assessment of passive safety systems reliability. Future work in Model-based Safety Analysis (MBSA) should focus on addressing the specific methodology relevant to safety systems. This should include addressing all the points mentioned in order to enhance the credibility of proposed approaches to address the issue and facilitate their endorsement by the scientific and technical community.

VI. CONCLUSION

A methodology has been developed to assess the reliability of passive systems, which are distinguished by three main components: systematic functional analysis, dynamic component analysis, and phenomenological factors. The dynamic methodology presented here overcomes the limitations of previous approaches by addressing the interaction between hardware/component failure and functional failure of passive systems, eliminating the need for separate analyses for each passive system and initiating events, and incorporating dynamic failures of components or processes. The inclusion of Monte Carlo simulation allows for the presentation of the influence of dynamic failure characteristics on system failure probability. As a result, the new methodology offers a more advanced form of probabilistic safety assessment (DPSA) and facilitates risk-informed decision making, leading to enhanced safety and reliability in nuclear power plant technology.

In order to resolve uncertainties in reliability calculations, which may arise due to assumptions about parameters such as atmospheric temperature, it is necessary to construct models of such parameters using data that has been continuously monitored during the application of passive systems. To incorporate these probability distributions into the Petri net analysis, a stochastic Petri net model is typically augmented with additional information, such as transition rates or probabilities, and then analysed using stochastic simulation techniques. The simulation generates a large number of sample paths, each representing a possible sequence of events and transitions, and calculates the likelihood of various outcomes based on these sample paths. Reliability estimations can be incorporated into Model-based Safety Analysis (MBSA) by using object-oriented languages [23] on addressing the specific methodology relevant to safety systems. The information can then be used to assess the overall safety of the system and identify areas where improvements can be made.

Furthermore, the next step would be incorporating the proposed methodology into GSPN model and try to apply the model with a case study associated with natural circulation phenomena in a passive safety system.

REFERENCES

[1] M. Ajmone-Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis, "Modelling with generalized stochastic Petri nets," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 26, no. 2, p. 2, 1995.

[2] *Safety Related Terms for Advanced Nuclear Power Plants*, document TEC-DOC-626, Sep. 1991.

[3] *Natural Circulation in Water Cooled Nuclear power Plants. Phenomena, Models, and Methodology for System Reliability Assessments*, document IAEA TEC DOC-1474, Nov. 2005.

[4] *Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants*, document IAEA TECDOC-1624, Nov. 2009.

[5] J. Jafari, F. D'Auria, H. Kazeminejad, and H. Davilu, "Reliability evaluation of a natural circulation system," *Nucl. Eng. Des.*, vol. 224, no. 1, pp. 79–104, Sep. 2003.

[6] B. Cai, Y. Zhang, H. Wang, Y. Liu, R. Ji, C. Gao, X. Kong, and J. Liu, "Resilience evaluation methodology of engineering systems with dynamic-Bayesian-network-based degradation and maintenance," *Rel. Eng. Syst. Saf.*, vol. 209, May 2021, Art. no. 107464, doi: 10.1016/j.ress.2021.107464.

[7] S. Baek and G. Heo, "Application of dynamic fault tree analysis to prioritize electric power systems in nuclear power plants," *Energies*, vol. 14, no. 14, p. 4119, Jul. 2021, doi: 10.3390/en14144119.

[8] V. Khare, S. Nema, and P. Baredar, "Reliability analysis of hybrid renewable energy system by fault tree analysis," *Energy Environ.*, vol. 30, no. 3, pp. 542–555, May 2019, doi: 10.1177/0958305X18802765.

[9] S. Kabir and Y. Papadopoulos, "Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review," *Saf. Sci.*, vol. 115, pp. 154–175, Jun. 2019.

[10] A. K. Nayak, V. Jain, M. R. Gartia, H. Prasad, A. Anthony, S. K. Bhatia, and R. K. Sinha, "Reliability assessment of passive isolation condenser system of AHWR using APSRA methodology," *Rel. Eng. Syst. Saf.*, vol. 94, no. 6, pp. 1064–1075, Jun. 2009.

[11] M. Marquès, J. F. Pignatel, P. Saignes, F. D'Auria, L. Burgazzi, C. Müller, R. Bolado-Lavin, C. Kirchsteiger, V. La Lumia, and I. Ivanov, "Methodology for the reliability evaluation of a passive system and its integration into a probabilistic safety assessment," *Nucl. Eng. Des.*, vol. 235, no. 24, pp. 2612–2631, Dec. 2005.

[12] *Procedures for Performing a Failure Mode, Effects, and Criticality Analysis*, Standard Mil-STD-1629a, 1980.

[13] D. H. Stamatis, *Failure Modes and Effects Analysis: FMEA From Theory to Execution*. Milwaukee, WI, USA: ASQC Quality Press, 1995.
[14] L. P. Pagani, G. E. Apostolakis, and P. Hejzlar, "The impact of uncertainties on the performance of passive systems," *Nucl. Technol.*, vol. 149, no. 2, pp. 129–140, Feb. 2005.
[15] *Potential Failure Mode and Effects Analysis (FMEA) Reference Manual*, 4th ed. General Motors Corporation, 2008.
[16] K. Hiromitsu and E. J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed. New York, NY, USA: IEEE Press, 1996.
[17] G. M. Koole, M. C. Van der Heijden, and R. H. Mak, "Dynamic fault trees: A comparison of approaches," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, pp. 207–218, doi: 10.1109/TPDS.2008.61.
[18] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree for fault-tolerant computer systems," *IEEE Trans. Rel.*, vol. 46, no. 3, pp. 372–382, 1997.
[19] P. Buchholz and A. Blume, "Dynamic fault trees with correlated failure times–modeling and efficient analysis," in *Proc. 41st Int. Symp. Reliable Distrib. Syst. (SRDS)*, Vienna, Austria, Sep. 2022, pp. 201–212.
[20] K. Aslansefat, S. Kabir, Y. Gheraibia, and Y. Papadopoulos, "Dynamic fault tree analysis: State-of-the-art in modeling, analysis, and tools," in *Reliability Management and Engineering: Reliability Management and Engineering*, H. Garg and M. Ram, Eds. Boca Raton, FL, USA: CRC Press, pp. 73–112.
[21] D. Vose, *Risk Analysis: A Quantitative Guide*, 3rd ed. Hoboken, NJ, USA: Wiley, 2008.
[22] K. D. Rao, V. V. S. S. Rao, A. K. Verma, and A. Srividya, "Dynamic fault tree analysis: Simulation approach," in *Simulation Methods for Reliability and Availability of Complex Systems* (Springer Series in Reliability Engineering). Cham, Switzerland: Springer, 2010, pp. 41–64.
[23] A. Zimmermann and T. Hotz, "Integrating simulation and numerical analysis in the evaluation of generalized stochastic Petri nets," *ACM Trans. Model. Comput. Simul.*, vol. 29, no. 4, pp. 1–25, Oct. 2019.
[24] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks," *Rel. Eng. Syst. Saf.*, vol. 71, no. 3, pp. 249–260, 2001, doi: 10.1016/S0951-8320(00)00077-6.
[25] Y. Papadopoulos, K. Aslansefat, P. Katsaros, and M. Bozzano, *Model-Based Safety and Assessment: 6th International Symposium, IMBSA 2019, Thessaloniki, Greece, October 16–18, 2019, Proceedings*. Cham, Switzerland: Springer, 2019.
[26] B. Bozzano and A. Cimatti, "Model-based safety analysis: An overview," *Int. J. Softw. Tools Technol. Transf.*, vol. 15, no. 3, pp. 195–202, 2013.
[27] M. Batteux, T. Prosvirnova, A. Rauzy, and L. Kloul, "The AltaRica 3.0 project for model-based safety assessment," in *Proc. 11th IEEE Int. Conf. Ind. Informat. (INDIN)*, Bochum, Germany, Jul. 2013, pp. 741–746, doi: 10.1109/INDIN.2013.6622976.

AKMALI MASOOD received the Ph.D. degree in nuclear physics from the University of Liverpool. He started his career with the University of Liverpool as a Teacher and also took on various assignments before joining the IAEA. During his tenure at the IAEA, he played an instrumental role in managing and supporting numerous research activities related to nuclear technology. In July 2022, he joined Assystem Energy and Operation, where he currently holds the position of Nuclear Safety Engineering Lead. He is also a highly qualified Physicist who graduated from the renowned University of Birmingham, U.K. His responsibilities include implementing innovative digitalized safety evaluation methodologies. His research interests include nuclear passive safety systems, reliability and validity evaluations, and integrating state-of-the-art reliability evaluation methodologies into model-based safety analysis (MBSA) and digital safety assessment analysis. He is a member of the Institute of Physics (IOP), U.K.

PLANA ROBERT (Senior Member, IEEE) received the Ph.D. degree in information and communication sciences and technologies. He has spent more than 30 years working in research and design, innovation, and digital transformation. After teaching for several years at the Paul Sabatier University of Toulouse and Institut Universitaire de France, he pursued a career in research and design and innovation management, holding various management positions with the CNRS, the French National Research Agency, and the French Ministry of Higher Education and Research. He continued his career in innovation with Alstom and GE where he oversaw various research and development programs in the field of smart grids and digital twins. He joined Assystem Energy and Operation, as the Chief Technology Officer, in 2017.