EVOLVING PSA METHODOLOGIES: TOWARDS DYNAMIC RELIABILITY IN SMR PASSIVE SYSTEMS

M. AKMALI, R. PLANA
ASSYSTEM
Paris, France
Email: makmali@assystem.com

FALAK SHER
DGB Technologies
Duisburg, Germany
Email: chfalak@dgbtek.com

Abstract

The evolution to Generation III+ and IV nuclear reactors, designed for reduced waste and enhanced safety, represents a significant advancement for Nuclear Industry in the context of Energy transition. Despite this, the lack of maturity and testing for these new technologies, especially in First of a Kind (FOAK) Demonstrator projects, presents challenges. Passive safety systems in these reactors are unfamiliar to regulatory bodies, making traditional Probabilistic Safety Assessment (PSA) methods inadequate. This paper addresses these challenges by introducing a novel dynamic approach to the reliability assessment of the Passive Isolation Condenser System (ICS) in Small Modular Reactors (SMRs), leveraging the SAFEST tool to enhance traditional PSA approaches. Through dynamic fault trees models, we incorporate probabilistic common cause failures, probabilistic dependencies, enhanced failure rates, failure-on-demand, addition of situation-based failure modes and failure ordering, leading to a more comprehensive and accurate evaluation of reactor safety. The integrated dynamic analysis not only covers the duration from the start of the reactor till 24 hours after a Loss of Coolant Accident (LOCA), but also utilises different failure modes for pre and post LOCA time periods. Moreover, it reveals that the system's reliability is highly sensitive to initial transient changes in pressure and temperature during post LOCA period. The results show that the frequency of core damage increases significantly when accounting for dynamic factors, offering a realistic and robust framework for nuclear safety assessment. This advancement highlights the importance of dynamic analysis in improving the reliability and safety of nuclear power plants, providing a detailed and realistic representation of their operational effectiveness, and contributing significantly to the field of nuclear safety.

1. INTRODUCTION

Reliability $R(t)$ is a measure of the dependability of safety of mission-critical systems, representing the probability of a system performing its required function within the time interval (0, t) [1]. Models based on fault trees, stochastic Petri nets, or Markov chains are commonly used to evaluate system reliability [1], providing insights into system behaviour, failure modes, and influencing factors, thereby aiding in system design, maintenance, and risk mitigation [2].

Dynamic systems, like nuclear passive safety systems, rely on physical phenomena such as natural convection, gravity, or phase change to safely shut down reactors and prevent radioactive release during accidents or power loss [2-4]. These systems are influenced by variables like temperature, pressure, and flow rates, and their performance involves uncertainties. Assessing their reliability requires understanding the physical phenomena through mathematical models, simulations, or experimental data.

Considering uncertainties and variability is crucial for the dependability of passive safety systems in advanced reactors, particularly SMRs. Despite advancements [5-8], challenges remain in incorporating passive systems into reactor designs and accurately quantifying their functional reliability under various conditions [2-4].

Recent research has introduced new reliability evaluation methodologies, enhancing understanding of system performance and resilience. Dynamic-Bayesian-network-based degradation and maintenance provide accurate predictions of system behaviour over time [6]. Availability-based resilience metrics offer new measures for informed decision-making, incorporating uncertainties and dependencies [7].

Researchers have explored static and dynamic fault trees for system analysis. Static fault trees model failure events, while dynamic fault trees capture redundancies, probabilistic dependencies, and failure ordering of events. Combining these models offers comprehensive reliability analysis. Studies by Baek, Sejin et al. [7] and Khare, Vikas et al. [7] proposed hybrid fault tree models to analyse system reliability comprehensively, improving

decision-making for system design, operation, and maintenance. These methodologies provide a comprehensive understanding of system performance and reliability, informing design, operation, and maintenance, thereby enhancing safety and reliability. Developing and applying these methodologies is essential for improving resilience to unforeseen events.

This study applies Dynamic Fault Trees (DFT) [9, 10] analysis to the isolation condenser system (ICS) driven by natural circulation, to provide emergency core cooling, residual heat removal, and pressure control of a prospective small modular reactor (SMR). Therefore, the current paper is organized as the following. After the introduction Section 2 reminds the Dynamic Fault Tree Analysis Method. In Section 3, it is presented the System selected to demonstrate the benefits of the method. Results are outlined in Section 4 when some conclusive remarks are given in the conclusion.

2. METHOD: DYNAMIC FAULT TREE ANALYSIS

The proposed methodology integrates dynamic behaviour into the static functional analysis of the system, incorporating phenomenological analysis. Systematic functional analysis methods like Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) [9] identify potential failure modes and their consequences in a structured manner. Based on the findings of FMEA, as compared to static fault trees, dynamic fault trees (DFT) modelling gives a more realistic and faithful models of the real-world systems. Their analysis [9-12] helps assess the reliability of individual components and their impact on overall system reliability. DFTs model the interactions between components over time, allowing for the calculation of probabilities for different failure scenarios. DFTs advance beyond traditional fault trees by incorporating dynamic gates such as Priority-AND (PAND), Spare (SPARE), and Functional Dependency (FDEP) as shown in Fig 1, which enable more faithful modeling of dependencies and event sequences. This approach is crucial for understanding dynamic system behaviours and enhances the accuracy of reliability assessments [11].

Figure 1 Commonly used logic gates in DFT – an extension of static fault trees.

The dynamic behaviour of a nuclear reactor includes its response to changes in operating conditions or abnormal events, such as a loss of coolant accident. Physical phenomena like heat transfer, fluid mechanics, and thermodynamics are crucial in determining system behaviour under these conditions. Therefore, safety studies of nuclear reactors must integrate both static and dynamic aspects and incorporate physical phenomena factors. Integrating dynamic fault tree analysis into static fault tree analysis offers several advantages, including (a) management of spare components, (b) allocation functional dependencies and (c) failure sequence ordering.

2.1. Specification of queries against dynamic fault trees

The semantics of dynamic fault trees (DFT) are given as Markov automata (MA) [21] – a generalization of continuous time Markov chains (CTMC) [15] with non-deterministic options at states --, which are analysed using state-of-the-art probabilistic model-checking techniques [21]. To address state-space explosion problem in the analysis of large DFTs, hybrid approaches are employed that analyse static parts of trees using BDDs-based approach, whereas dynamic parts are analysed using Markov analysis.

The generated MA from DFTs are analysed using probabilistic model-checking against reliability measures defined in continuous stochastic logic (CSL) with reward extensions [19]. Sets of states in MA are described by Boolean combinations over the state labelling's, i.e., failed and operational events in DFTs. The following two standard CSL properties are the building blocks for the reliability queries as discussed in [20].

a) Reach-avoid probability. Given a state $s \in S$, a set of target states and a set of bad states, the property Ps (bad U target) describes the probability to eventually reach a target state from state *s* without visiting a bad state in-between. If the set of bad states is empty, the reach-avoid probability reduces to Ps (F target), and is just a reachability probability.
b) Time-bounded reach-avoid probability. Incorporating an additional timebound t, the property Ps (bad U <= t target) describes the probability to reach a target state (while avoiding bad states) from

state *s* within timebound *t*. Similar as before the time-bounded reachability is described by Ps (F <= t target).

As discussed in Ref [20], the reliability measures, for the integrated analysis of pre and post LOCA duration as well as full functional availability after LOCA, are based on the following model-checking queries. The atomic proposition *failed* denotes states where the top-level event in the FT has failed and *degraded* denotes states when a specific event, e.g. *LOCA, Comp A* failed, etc. has already occurred.

a) Full Function Availability (FFA) – $1 - P(F \leq t\ failed\ |degraded)$ -- describes the time-bounded probability that the system provides full functionality, i.e., neither it has failed, nor event *degraded* (e.g. LOCA) has occurred till the timebound *t*. It is described as the complement of the time bounded reachability of a *failed* or *degraded* state.
b) Failure Without Degradation (FWD) – $P\ (!\,degraded\ U \leq t\ (!\,degraded\ \&\ failed))$ -- describes the time-bounded probability that the system fails without being degraded first (or e.g. without occurrence of LOCA). It is the time-bounded reach-avoid probability of reaching a failed state without reaching a degraded state.
c) Failure under Limited Operation in Degradation (FLOD) -- $\sum_{s \in degraded}(P(!\,degraded\ U \leq t\ s) * Ps\ (F \leq t\ drivecycle\ failed))$ -- describes the probability of failure when imposing a time limit for using a degraded system. For all degraded states the time-bounded reachability probability of a failed state is computed within the restricted time-bound given by a drive cycle. This value is scaled by the time-bounded reach-avoid probability of reaching a degraded state without degradation before.

2.1.1 *Development of Failure Rates for Valves and Heat Exchangers Due to Transient Parameters*

The reliability of Valves and heat exchangers can be significantly affected by transient operational parameters like temperature and pressure. To accurately assess their reliability, we developed models that incorporate the sensitivity of these components to changes in these parameters.

2.1.1.1 Failure Rate Model for Heat Exchangers

Heat exchangers' failure rates are influenced by deviations from their optimal operating conditions, specifically temperature and pressure. The adjusted failure rate (λ') for heat exchangers derived from empirical data and Monte Carlo simulations from [18] is modeled as:

$$\lambda' = \lambda \times \left(1 + k_T \frac{\Delta T}{T_{\text{steady}}} + k_P \frac{\Delta P}{P_{\text{steady}}}\right) \quad (1$$

Where λ : The original failure rate. ΔT: The absolute deviation from the steady-state (optimal) temperature. ΔP: The absolute deviation from the steady-state (optimal) pressure. T_{steady}: The steady-state temperature. P_{steady}: The steady-state pressure. k_T: Sensitivity factor for temperature changes k_P: Sensitivity factor for pressure changes. The sensitivity factors are derived from the analytical works done by Ref [18].

2.1.1.2 Failure Rate Model for Valves

The reliability of valves is affected by both temperature and pressure variations [19, 20]. The total unreliability rate (λ_{total}) for valves based on the experimental study conducted in Ref [19, 20] is modeled as:

$$\lambda_{\text{total}} = \lambda_0 \times e^{\frac{E_a}{k}\left(\frac{1}{T_{\text{ref}}} - \frac{1}{T}\right)} \times (1 + \alpha \Delta P) \quad (2$$

where λ_0: The base failure rate. E_a: Activation energy, indicating the sensitivity of the failure rate to temperature changes. k: Boltzmann's constant. T_{ref}: The reference temperature. T: The operating temperature. α: Sensitivity factor for pressure changes. (ΔP): The relative pressure change calculated as $(\frac{P_{\text{transient}} - P_{\text{baseline}}}{P_{\text{baseline}}})$.

This model incorporates the exponential relationship between temperature and failure rate, as well as the linear relationship between pressure changes and failure rate, providing a comprehensive assessment of valve reliability under different operational conditions.

2.1.1.3 A comprehensive DFT modeling of a reactor

Unlike previous reliability analysis study using RiskSpectrum tool [17], in this work a more faithful model of the system is built using DFTs by incorporating the following: (a) modeling LOCA as a BE with a failure rate

that triggers other events on its occurrence, (b) incorporating failure-to-open/close failure modes e.g. failure to open/close a valve at LOCA , (c) having new failure modes in the post LOCA scenarios e.g. valve rupture failure mode , (d) having increased failure rates during the post LOCA scenarios e.g. increased failure rate of piping, and (e) having temperature/pressure dependent failure rates of valves. We computed the cumulative probability of failure of the reactor for the duration starting from the start of the reactor till 24 hours after the occurrence of LOCA for the highest temperature and pressure. Thanks to DFTs that allow us to have different failure rates/failure modes during the pre LOCA duration and 24 hours after the LOCA. Moreover, we also analysed the impact of temperature and pressure on the full availability of the reactor in discrete intervals after LOCA. The analysis shows the real dynamic response of the system to such accidents and obtain a realistic view of its reliability. This approach provides a more comprehensive and accurate evaluation of reactor safety by considering both the availability of the system under normal conditions and its reliability under accident conditions.

In the current study, the SAFEST Tool [18] is used to dynamically assess the reliability of BWRX-300. The SAFEST tool, developed by DGB Technologies in collaboration with Twente and RWTH Aachen universities [18], revolutionises nuclear reactor safety analysis by combining advanced analytical techniques with user-friendly interfaces. It offers BDD, Markov, and hybrid analysis for DFTs, supports complex measure specifications using PCTL/CSL logics. It enhances classical event trees with embedded DFTs for comprehensive system reliability assessment. SAFEST event trees extend classical ETs with (a) state rewards/losses, and (b) non-deterministic decision-making at states. Their analysis using probabilistic model-checking provides upper & lower bounds on the probabilities/frequencies of consequences, and expected values of different quantities of interest e.g. radionuclide emission, etc. Moreover, the analysis helps figuring out what specific sequence of decisions, after the bad event, will e.g. minimize the probabilities/frequencies of dangerous consequences in stochastic environment.

3. CASE STUDY: THE BWRX-300 SMALL MODULAR REACTOR

The BWRX-300 [16, 17] is a Generation III+ small modular, light water reactor with a power output of approximately 300 MWe. Developed by GE Hitachi Nuclear Energy (GEH) [16], it represents the tenth generation of the Boiling Water Reactor (BWR) series and is a small modular evolution of the previous Economic Simplified Boiling Water Reactor (ESBWR). The BWRX-300's innovative features and increased reliance on passive safety systems make it an ideal candidate for assessing passive reliability and performing a Level 1 probabilistic safety assessment [18]. While the core design of the BWRX-300 remains conventional, significant design changes revolve around reducing the complexity of safety systems including reactor Pressure Vessel (RPV) Isolation Valves and removal of Safety Relief Valves [16].

The BWRX-300 utilizes two passive cooling systems: the Isolation Condenser System (ICS) and the Passive Containment Cooling System (PCCS). This study focuses on the ICS. The ICS manages residual heat removal and emergency pressure control for the BWRX-300. It consists of three independent loops, each capable of 100% decay heat removal capacity. Heat is transferred through natural circulation from the steam in the RPV head to a condenser pool, where it condenses and returns to the vessel. Water in the condenser pool evaporates and discharges to the atmosphere, acting as the ultimate heat sink. The combined capacity of the IC pools ensures heat removal for seven days, with indefinite capability if water is replenished [5]. A diagram of the ICS is provided in Figure 2.

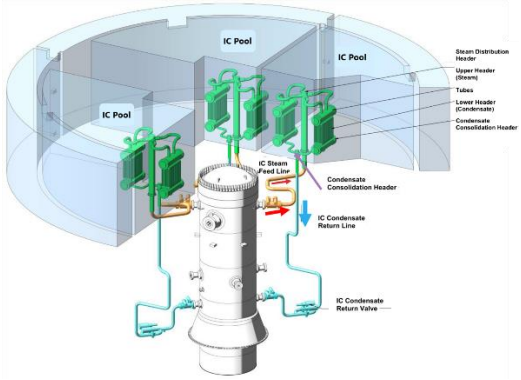


Figure 2 Diagram of the Isolation Condenser System, [16].

Probabilistic Safety Assessment (PSA) [18] is used to quantify the risk associated with a technology by assessing the frequency or severity of potential consequences. Originally developed in the aerospace industry, PSA is now widely used in nuclear engineering to evaluate hazards and the effects of plant modifications on safety. As safety metrics improve, PSA increasingly focuses on evaluating relative differences in these metrics rather than their absolute values. This study focuses on Level 1 PSA, which may consider both internal and external initiating events and delineate by the reactor's operational state (full power or shutdown).

4. RESULTS

In this study, a partial Level 1 Probabilistic Safety Assessment (PSA) was conducted for the BWRX-300 reactor, focusing on an internal initiating event—specifically, a Loss of Coolant Accident (LOCA) occurring at full power. For the purposes of this analysis, the LOCA event, as categorized in NUREG/CR-6928 [18], was selected as the primary initiating event. Although LOCAs are further sub-categorized by factors such as location/type (e.g., liquid, steam, below top of fuel), break size, the ability of the break to depressurize the Reactor Pressure Vessel (RPV), and whether the break falls within the capacity of the Control Rod Drive (CRD) injection system, this study primarily considers the overall LOCA event (including the small, medium and large LOCA). This was accomplished by developing Dynamic Fault Trees (DFTs), which were subsequently quantified using Markov Automata within the SAFEST tool.

The DFTs are developed for Reactor Isolation System (RIS), Reactor Scram (RS), Boron Injection System (BIS) and Isolation Condenser System (ICS), then calculated their reliability within 24 hours after LOCA. Finally, an event tree is built integrated with DFTs of RIS, RS and ICS to analyse frequencies of different consequences. Only the ICS analysis is discussed in the following sections. Failure rates are taken from NRC-licensed ESBWR [17]. The DFT of ICS system is built based on the static fault tree from Hitachi [16] and [17] and later. is extended with additional dynamic features as:

a) Failure to Open on Demand (FOD): The FOD is included for valves V5 & V6 for all the loops A, B and C, addressing scenarios where valves fail to open when needed, affecting the ICS system's reliability at the occurrence of LOCA.
b) Common Cause Failure (CCF): The analysis considers CCF for valves V5 (V6) in loops A, B and C as well as CCF for heat exchangers, accounting for simultaneous failures due to a shared cause, which is critical for accurately assessing system reliability [17].
c) Additional Failure Modes (AFM): The added new failure modes, such as valve rupture rates for V1, V2, V3, V4, V5 and V6 for loops A, B and C, to capture potential mechanical failures during post LOCA period, providing a more comprehensive view of system vulnerabilities.
d) Increased Failure Rates: The failure rates of heat exchangers as well as pipings in loops A, B and C are increased during the post LOCA period, addressing scenarios where failure rates of components increased when they are operational.

DFT of Loop A in ICS without incorporating the above features is shown in the Figure 3, where the DFT of the whole ICS after incorporating CCFs and dependencies has 154 basic events, 93 static gates and 39 dynamic gates and cannot be displayed here.

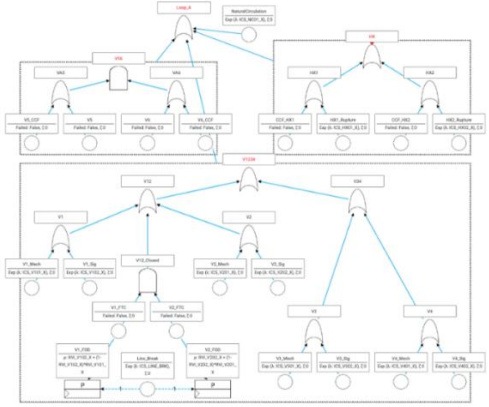


Figure 3 Fault Tree of ICS without incorporating CCF and probabilistic dependencies.

The Figure 4 illustrates the probability of failure of the Reactor Isolation (ICS) system within 24 hours of LOCA as a function of the time in years when the LOCA occurs. The x-axis represents the number of years until a LOCA might occur, while the y-axis shows the corresponding failure probability of the ICS system within the first 24 hours after the LOCA. The graph reveals that as the reactor ages, the probability of the ICS system failing within 24 hours of a LOCA steadily increases. This trend underscores the impact of component aging and degradation over time, highlighting the necessity for dynamic reliability assessments that account for these changes. Unlike static models, which assume constant failure rates, this approach provides a more accurate depiction of system reliability, emphasizing the need for continuous monitoring and proactive maintenance to ensure sustained safety and performance throughout the reactor's operational life.

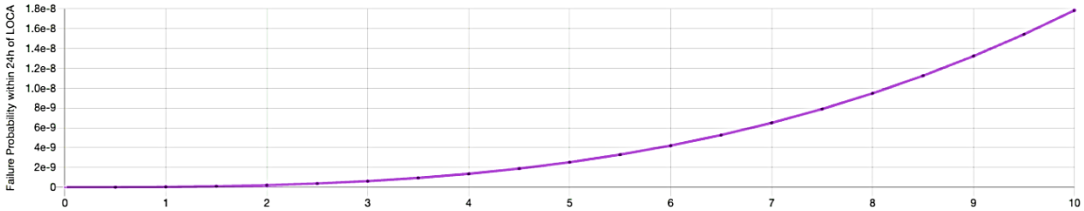


Figure 4 Probability of failure of ICS within 24h after LOCA.

The full functional availability of the ICS after a LOCA under time-dependent temperature and pressure conditions, which is assumed to be constant in 0.15 min interval, is illustrated in Figure 5. It is assumed that the system is fully functional at the beginning of each analysis interval of 0.15 min. It reveals important insights into the system's dynamic behaviour. Initially, when the LOCA occurs, the reactor experiences a significant transient phase characterized by sharp increases in pressure and temperature, as shown in the attached graphs. These high initial values stress the system components, leading to an elevated failure rate during the early moments of the 24-hour cycle.

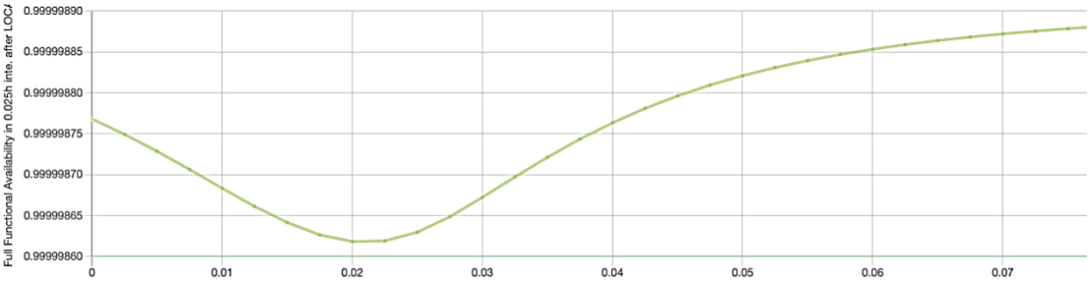


Figure 5 Full Functional Availability of ICS After LOCA in Intervals (assuming full system availability at the beginning of 0.15 min interval in which temperature & pressure is assumed to be constant).

The plot shows a slight initial decrease in the availability of the ICS, reaching a minimum before gradually increasing. This initial dip can be attributed to the immediate impact of the transient conditions on system components, such as valves and heat exchangers, which are more likely to fail when subjected to abrupt pressure and temperature changes. As time progresses, the system begins to stabilise, and the availability starts to improve. This recovery highlights the system's ability to adapt and restore functionality even under the challenging conditions following a LOCA.

DFT of Reactor Isolation System: Before and after incorporating all CCFs and dependencies, the final DFT is shown in the Fig. 6 (enlarged in Appendix A).

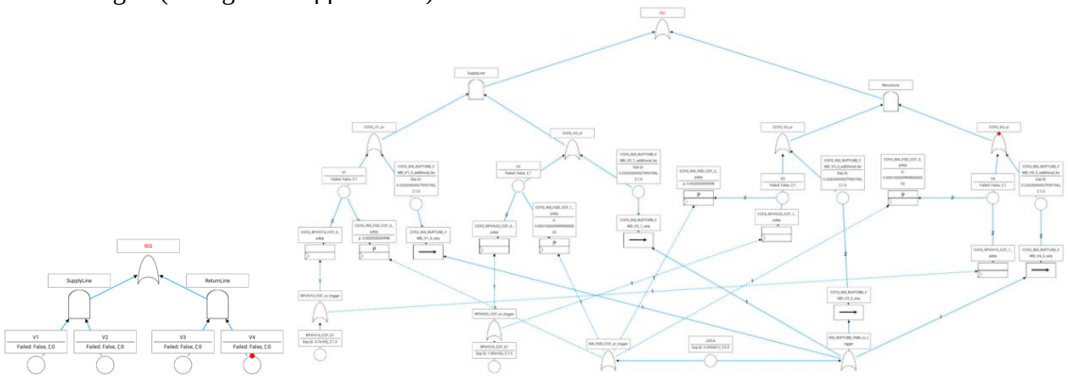


Figure 6 Static fault tree (left) of DFT (right) of Reactor Isolation System

Reward Event Tree of LOCA is illustrated in the Fig. 7 (enlarged in Appendix B). The Reward Event Tree (RET) for a Loss of Coolant Accident (LOCA), provides a detailed overview of potential outcomes following a LOCA in a Small Modular Reactor (SMR). The tree begins with the LOCA event and traces the possible paths based on the success or failure of critical systems, such as the Residual Heat Removal System (RS).

Figure 7 Dynamic Event Tree of LOCA

If the initial response to the LOCA is successful, the event tree branches towards less severe outcomes, like "CoreDamage_C3," indicating minimal core damage. However, if critical systems fail, the tree shows a progression to more severe core damage scenarios, with "CoreDamage_C1" representing the most significant damage. The tree demonstrates how the reliability of each system directly influences the severity of the outcomes. Successful operation of key systems can prevent or minimise core damage, while failures increase the likelihood of severe consequences. The probabilities attached to each branch offer a quantitative assessment, highlighting the importance of maintaining system reliability to reduce the risk of severe core damage in a LOCA event.

The detailed consequence analysis for event sequences leading to core damage was conducted using SAFEST. While the frequency of a LOCA event is estimated at 4.21E-4 per year [17], Table I highlights the likelihood of varying levels of core damage. Category 1 (CoreDamage_C1) represents the most severe core damage (100%), Category 2 (CoreDamage_C2) indicates medium severity (50%), and Category 3 (CoreDamage_C3) reflects the least severe damage (10%). Each category is associated with a corresponding frequency, illustrating the relative probabilities of these outcomes.

TABLE I Consequence Frequencies (Duration of LOCA: 1year and its freq: 0.000421).

Consequence	Expected Frequency (yr $^{-1}$)
CoreDamage_C1	1.34E-8
CoreDamage_C2	5.13E-13
CoreDamage_C3	6.55E-9

Table I shows the results of the SMR LOCA analysis. Over a one-year period, the probabilities of minor, moderate, and severe core damage are exceedingly low, with expected frequencies of 1.34E-8, 5.13E-13, and 6.55E-9, respectively.

The table provides an analysis of potential core damage scenarios following a Loss of Coolant Accident (LOCA) in a Small Modular Reactor (SMR), categorizing them by severity and estimating their likelihood. The first scenario, "CoreDamage_C1," represents minor core damage with an extremely low probability of 1.34×10^{-8} per year, indicating it is highly unlikely to occur. The next, "CoreDamage_C2," involves more severe damage, with an even lower likelihood of 5.13×10^{-13} per year, making it exceedingly rare. The most severe outcome, "CoreDamage_C3," which entails significant core damage, has a frequency of 6.55×10^{-9} per year. Despite being the most serious, it remains highly improbable. Overall, the table illustrates that while core damage is possible in a LOCA event, the likelihood of such occurrences is extremely low, especially for the more severe scenarios.

Additionally, Table II, outlines the expected losses in terms of casualties, radionuclide release, and contaminated land. The current dynamic PSA estimates minimal expected losses, with exceptionally low probabilities of significant casualties or environmental impact, using the statistical data of casualties reported from the Chernobyl accident as reported by IAEA [22].

Table II Expected Losses (based on data taken from Chernobyl accident [22])

Losses	Expected Value
Casualties	8.01E-7 Lives
Radionuclide	3.14E-6 Million Curries
Contaminated Land	1.74E-5 Sq miles

As shown in Table II, the analysis predicts an extremely low impact in terms of expected losses. The expected number of casualties is 8.01E-7 lives, indicating that the risk to human life is negligible. The potential release of radionuclides is minimal, with an expected value of just 3.135E-6 million curies, and the expected land contamination is similarly low, at 1.735E-5 square miles.

5. DISCUSION

The results from the traditional Probabilistic Safety Assessment (PSA) performed using the RiskSpectrum tool for the BWRX-300 [17], yield a core damage frequency (CDF) of 1.23E-07 per year [17]. This value reflects the system's reliability under the assumption of traditional analysis, focusing on internal initiating events at full power, including the potential failure of components like valves and heat exchangers, but without explicitly modeling transient conditions.

In comparison, our dynamic PSA approach, which estimates a total core damage frequency of approximately 1.996E-08 per year, provides a more granular analysis. Although our analysis did not include all potential initial events such as transients or vessel rupture, it did incorporate the failure rates of valves and heat exchangers due to transient parameters. This approach allows us to account for the indirect effects of transient conditions on system failure, which may not be fully captured in the traditional PSA.

The significantly lower core damage frequency obtained in our dynamic PSA suggests that the inclusion of transient-related failure rates, even without considering all possible initial events, provides a more conservative estimate of the system's reliability. However, it's important to note that this lower frequency does not imply a broader safety margin unless the full spectrum of initiating events is considered. The traditional PSA provides a more comprehensive view by considering a wider range of scenarios, but our dynamic approach offers a focused analysis that may highlight specific vulnerabilities related to transient conditions that are not as explicitly addressed in the traditional method.

The results of the dynamic event tree analysis show that the expected frequencies for core damage scenarios under the dynamic model are more varied and detailed compared to the static model. For example, this study found a lower frequency of core damage in certain scenarios, due to the realistic modeling of system responses and failure mechanisms over time. Additionally, the expected losses in terms of casualties, radionuclide release, and contaminated land area were meticulously calculated, providing a comprehensive risk assessment.

This dynamic approach also incorporates thermohydraulic parameters obtained from previous study [17], blending deterministic and probabilistic assessments to achieve a hybrid methodology. This ensures that the evaluation is not only probabilistic but also grounded in the physical realities of the reactor's operation, making it a highly realistic assessment of system safety. The integration of dynamic safety assessment methods into the fault tree analysis for SMR reactors provides a more accurate and realistic evaluation of system reliability compared to traditional static methods.

6. CONCLUSION

The current study introduces a dynamic safety assessment methodology for the Small Modular Reactor (SMR) Isolation Condenser System (ICS), offering a significant advancement over traditional static analysis methods offered by tools such as RiskSpectrum [17]. By incorporating time-dependent failure rates and system responses to transient conditions, the dynamic approach provides a more realistic evaluation of system reliability.

Nevertheless, a comprehensive interpretation of risk assessment outcomes necessitates the integration of these results with uncertainty quantification. Additionally, performing sensitivity analysis is crucial to identifying particularly vulnerable components in the design and evaluating the confidence level in the assessment's conclusions. In the context of the Dynamic Probabilistic Safety Assessment (DPSA) discussed in this study, executing such an analysis requires a thorough understanding of various criticality metrics, including the Diagnostic Importance Factor, Risk Achievement Worth, and Risk Reduction Worth. Consequently, future research will involve sensitivity studies where multiple appropriate time intervals are selected for all critical components. This approach will facilitate a comparative analysis, allowing for the comparison of results obtained from dynamic PSA with those derived from traditional PSA.

REFERENCES

[1] JAFARI, J. D'AURIA, F. KAZEMINEJAD, H. DAVILU, H. Reliability evaluation of natural circulation system. Nucl. Eng. Des. 2003, 224,79–104

[2] IAEA, TEC-DOC-626, 1991. Safety related terms for advanced nuclear power plants. September 1991.

[3] IAEA TECDOC-1624, 2009. Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants. November 2009

[4] BAOPING CAI, YANPING ZHANG, HAIFENG WANG, YONGHONG LIU, RENJIE JI, CHUNTAN GAO, XIANGDI KONG, JING LIU, (2021). Resilience evaluation methodology of engineering systems with dynamic-Bayesian-network-based degradation and maintenance. Reliability Engineering; System Safety,

[5] BAEK, SEJIN & HEO, GYUNYOUNG. (2021). Application of Dynamic Fault Tree Analysis to Prioritize Electric Power Systems in Nuclear Power Plants. Energies. 14. 4119. 10.3390/en14144119.

[6] KHARE, VIKAS & NEMA, SAVITA & BAREDAR, PRASHANT. (2018). Reliability analysis of hybrid renewable energy system by fault tree analysis. Energy & Environment. 30.

[7] NAYAK, A.; JAIN, V.; GARTIA, M.; PRASAD, H.; ANTHONY, A.; BHATIA, S.; SINHA, R. Reliability assessment of passive isolation condenser system of AHWR using APSRA methodology. Reliab. Eng. Syst. Saf. 2009, 94, 1064–1075.

[8] MARQUÈS, M.; PIGNATEL, J.; SAIGNES, P.; D'AURIA, F.; BURGAZZI, L.; MÜLLER, C.; BOLADO-LAVIN, R.; KIRCHSTEIGER, C.; LA LUMIA, V.; IVANOV, I. Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment. Nucl. Eng. Des. 2005, 235, 2612–2631.

[9] G. M. KOOLE, M. C. VAN DER HEIJDEN, AND R. H. MAK, "dynamic fault trees: a comparison of approaches," Ieee transactions on reliability, vol. 46, no. 3, pp. 372-382, 1997.

[10] P. BUCHHOLZ AND A. BLUME, "Dynamic Fault Trees with Correlated Failure Times - Modeling and Efficient Analysis -," 2022 41st International Symposium on Reliable Distributed Systems (SRDS), Vienna, Austria, 2022, pp. 201-212.

[11] ASLANSEFAT, KOOROSH & KABIR, SOHAG & GHERAIBIA, YOUCEF & PAPADOPOULOS, YIANNIS. (2020). Dynamic Fault Tree Analysis: State-of-the-Art in Modelling, Analysis and Tools.

[12] VOLK, M., SHER, F., KATOEN, J.-P., AND STOELINGA, M. 2024. SAFEST: Fault Tree Analysis Via Probabilistic Model Checking. Annual Reliability and Maintainability Symposium (RAMS), Albuquerque, NM, USA, pp. 1-7.

[13] HASSAN AZARKISH, MOHSEN RASHKI, Reliability and reliability-based sensitivity analysis of shell and tube heat exchangers using Monte Carlo Simulation, Applied Thermal Engineering, Volume 159, 2019, 113842, ISSN 1359-4311,

[14] SUN-KI LEE, Performance Analysis of Air Operated Valve by Thermal Aging, Journal of the Korean Society for Power System Engineering, Vol. 19, No. 5, pp. 93-98, October 2015

[15] YUAN, G.; WANG, Y.; YANG, X.; FANG, Y.; MA, R.; NING, K.; GUAN, M.; TANG, Y. Study on Quantitative Evaluation Method for Failure Risk Factors of the High-Temperature and High-Pressure Downhole Safety Valve. Sustainability 2024, 16, 1896.

[16] GE Hitachi Nuclear Energy, ESBWR CERTIFICATION PROBABILISTIC RISK ASSESSMENT, NEDO-33201 Revision 6. GE-Hitachi Nuclear Energy Americas LLC, 2010

[17] GRAEME TRUNDLE, Reliability Assessment of Passive ICS in an SMR as part of the PSA Analysis, SH204X Master Thesis Report, 2023

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Defining Initiating Events for Purpose of Probabilistic Safety Assessment. in TECDOC Series, no. 719. Vienna: 1993.

[19] Baier C, Hahn EM, Haverkort BR, Hermanns H, Katoen J-P. Model checking for performability. Math Struct Comput Sci 2013;23(4):751–95.

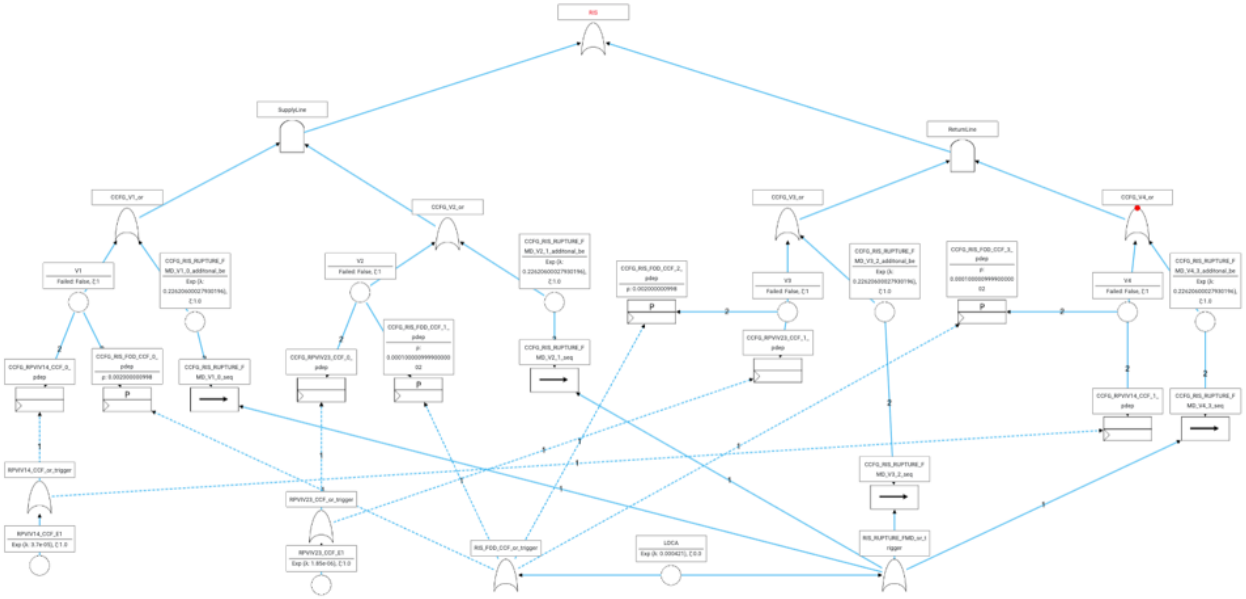
[20] Ghadhab M, Junges S, Katoen JP, Kuntz M, Volk M. Safety analysis for vehicle guidance systems with dynamic fault trees. Reliability engineering & system safety. 2019 Jun 1;186:37-50.

[21] Volk M, Junges S, Katoen J-P. Fast dynamic fault tree analysis by model checking techniques. IEEE Trans Industr Inf 2018;14(1):370–9.

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Environmental Consequences of the Chernobyl Accident and their Remediation:Twenty Years of Experience. radiological assessment reports series 2006

APENDIX

A: DFT of Reactor Isolation System



B : Dynamic Event Tree of LOCA