Advances in Reliability, Safety and Security, Part 1 – Kołowrocki, Dąbrowska (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-13-5 (printed), ISBN 978-83-68136-00-5 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Advancing Nuclear Reactor Safety Analysis: Methodological Innovations And Results From Dynamic Probabilistic Safety Assessment

Masood Akmali[a], Falak Sher[b]

[a]Assystem Engineering & Operation Services, Courbevoie, France
[b]DBG Technologies, Duisburg, Germany

Abstract

In advancing the field of nuclear safety, our study leverages Dynamic Probabilistic Safety Assessment (DPSA) techniques, utilizing dynamic fault trees (DFTs) and Markov models, to delve into the nuanced behaviors and potential failure modes within a nuclear reactor system. This methodology enables an intricate modeling of the temporal and probabilistic dependencies among system components, particularly focusing on the evaluation of Loss of Coolant Accident (LOCA) scenarios. By quantifying the probabilities of occurrence alongside the expected frequencies of core damage and radiological releases, we provide a detailed, time-dependent risk profile of the reactor's operations. Our findings offer critical insights into reactor safety, revealing a significant variance in the expected frequency of core damage in relation to operational time. Notably, we identified a peak risk at 20,000 hours of operation. Through sensitivity analysis, our study demonstrates a potential increase in core damage frequency—up to six times higher—with a sixfold increase in the failure rate of the Pool Isolation System (PIS), highlighting its crucial role in maintaining overall safety. Furthermore, uncertainty analysis sheds light on the impact of operational uncertainties in the Emergency Core Cooling System (ECCS), where a 20% uncertainty can alter the core damage frequency by nearly 10%. These analyses underscore the importance of ECCS reliability in effectively mitigating LOCA consequences. Our work demonstrates the potential of DPSA methodologies to provide precise, time-sensitive evaluations of nuclear safety risks, enabling the development of more robust and informed safety strategies. This comprehensive assessment approach promises significant advancements in the proactive management and mitigation of risks in nuclear reactor systems.

Keywords: dynamic probabilistic safety assessment, nuclear reactor safety, dynamic fault trees, Markov models

1. Introduction

Reliability, represented as $R(t)$, is pivotal for assessing the dependability of critical systems, defined as the probability of a system performing its required function in a specific period $(0, t)$. Analytical models based on fault trees, stochastic Petri nets, or Markov chains are utilized to predict reliability and understand system dynamics and failure mechanisms, aiding in design and risk management decisions (Ajmone-Marsan, 1995). With advancements in reactor technology, ensuring the reliability of passive safety systems under various operational conditions has become a key focus, necessitated by technological advances and regulatory demands (Jafari, 2003; Khare, 2018). These systems' reliability significantly depends on component integrity and performance across all scenarios (IAEA, 1991, 2009). Recent research introduces dynamic Bayesian networks and availability-based engineering resilience metrics to improve system behavior and resilience understanding (Baoping, 2021; Baek, 2021). Hybrid models combining static and dynamic fault trees offer a comprehensive view of system reliability, considering both immediate and temporal behaviors and the impact of maintenance (Zhang, 2020). Such methodologies enhance decision-making for system design and maintenance, boosting system safety and reliability. This shift towards dynamic methodologies for reliability evaluation addresses the limitations of static models, offering a nuanced, adaptable approach to safety assessment in line with evolving reactor technologies.

This advancement aims to provide an accurate reflection of operational risks, promoting informed decisions and upholding safety commitments. Another research initiative by (Khare, et al. 218) adopted a similar hybrid approach for the reliability analysis of a hybrid renewable power station. This approach underscores the potential of hybrid static-dynamic fault tree models to furnish a comprehensive perspective on system reliability, accounting for the multifaceted static and dynamic attributes of the system. Such an approach not only enhances decision-making processes concerning system design, operation, and upkeep but also bolsters the overall safety and dependability of engineering systems.

The development of this dynamic methodology for reliability evaluation in the nuclear sector is driven by the necessity to enhance the precision and adaptability of safety assessments. Recognizing the limitations of static models in capturing the complex, time-varying behavior of reactor systems, this new approach integrates dynamic interactions and probabilistic analyses to provide a nuanced and responsive risk assessment tool. Motivated by the need for advanced safety strategies that keep pace with evolving reactor technologies, this methodology aims to deliver a more accurate, comprehensive understanding of operational risks, supporting informed decision-making and reinforcing the industry's commitment to safety.

The methodologies described herein amalgamate the static and dynamic dimensions of system analysis, paving the way for a deeper understanding of system performance and reliability. These methodologies play a crucial role in shaping the design, operational strategies, and maintenance protocols of engineering systems, ultimately elevating their safety and resilience against unforeseen challenges.

2. Methodology for safety system reliability analysis

This innovative methodology for assessing the reliability of safety systems, inclusive of passive mechanisms, marks a pivotal advancement in nuclear safety and risk evaluation. Diverging from conventional practices, our approach synthesizes three principal components: systematic functional analysis, dynamic component scrutiny, and the incorporation of phenomenological considerations. By melding these facets, the methodology provides a nuanced and authentic evaluation of passive system reliability, accounting for the dynamic interplay of system behaviors and the impact of diverse external influences. This dynamic methodology remedies prior limitations, such as overlooking the interaction between hardware failures and functional inadequacies of passive systems, the necessity for isolated analyses across different passive systems and initiating events, and the challenges in capturing dynamic failures. The methodological integration of Monte Carlo simulations illuminates the dynamic failure characteristics of components, enriching the probabilistic safety assessment (DPSA) landscape and fostering risk-informed decision-making, thereby enhancing the safety and dependability of nuclear power technologies.

2.1. Static and dynamic system aspects of safety analysis

A nuclear reactor's safety analysis necessitates a balanced consideration of both static and dynamic system elements alongside physical phenomena factors. The static domain encompasses the reactor's design, materials, and geometry—foundational elements that dictate system behavior under standard operations. Conversely, the reactor's dynamic responses to operational shifts or abnormal events, governed by principles of heat transfer, fluid dynamics, and thermodynamics, are equally critical to its safety profile.

The fusion of dynamic fault tree analysis into the conventional static fault tree framework introduces a multifaceted approach to reliability analysis, offering significant advantages in understanding and optimizing system reliability, particularly in nuclear safety systems. This integration addresses several critical aspects:

- Management of Spare Components and Allocation;
- Functional Dependency;
- Failure Sequence Dependency.

Transitioning from static models to Dynamic Fault Tree (DFT) analysis marks a leap forward in reliability modeling, capturing dependencies between components that static models overlook. By mapping the entire state space and adopting Continuous Time Markov Chain (CTMC) techniques, this dynamic approach offers a sophisticated representation of system reliability. Incorporating factors beyond the mechanical—like human error, environmental influences, and operational challenges—enriches the evaluation, guiding decision-making for system design, maintenance, and risk mitigation with greater accuracy and depth.

2.2. Methodological framework for nuclear reactor safety analysis using DFT and DET approaches

The cornerstone of our safety analysis is the development of Dynamic Fault Trees (DFTs), sophisticated models designed to capture the complex interplay and temporal behaviors of components within a nuclear reactor system. DFTs advance beyond traditional fault trees by incorporating dynamic gates—Priority-AND (PAND), Spare (SPARE), and Functional Dependency (FDEP) as shown in Figure 1 —which facilitate intricate modeling of dependencies and event sequences critical to understanding dynamic system behaviors. This essential phase ensures a thorough grasp of the dynamic interactions within the reactor system, where the sequence and timing of component failures are pivotal to assessing overall system safety.

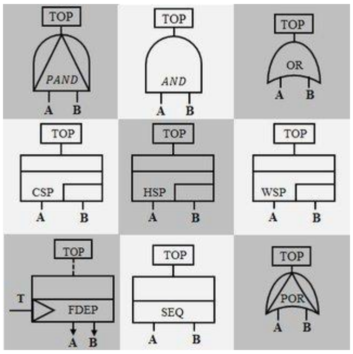


Fig. 1. Commonly used logic gates in DFT.

The methodology advances reliability assessment by translating Dynamic Fault Trees (DFTs) into Continuous Time Markov Chains (CTMCs) for an in-depth evaluation of reactor behavior across varied scenarios. Model checking rigorously verifies the CTMC against safety standards, identifying risks and ensuring system integrity. This process is streamlined with Binary Decision Diagrams (BDDs) for efficient analysis and bolstered by modularization for manageability. Combining DFTs with Dynamic Event Tree (DET) analysis enriches the safety strategy with scenario-driven insights. These methods collectively offer a comprehensive safety overview, informing decisions for system enhancement and risk management.

The SAFEST tool (Volk, 2024; Verma, 2021) has been used to follow our methodology, enabling a rigorous examination of the nuclear reactor's safety systems through a detailed probabilistic lens.

3. SAFEST Tool

The SAFEST tool developed jointly Twente and RWTH Aachen (Volk, 2024) by represents a paradigm shift in the analysis and assessment of nuclear reactor safety. It amalgamates advanced analytical techniques with user-friendly interfaces, making it an indispensable asset for both researchers and practitioners in the field. The SAFEST incorporates a blend of analytical techniques to assess system reliability comprehensively:

- BDD, Markov, and Hybrid Analysis: By combining binary decision diagrams (BDD) for static fault trees and state-based techniques for dynamic fault trees (DFT), SAFEST offers a hybrid analysis approach that significantly outperforms traditional methods.
- Specification of Complex Measures: Utilizing probabilistic computational tree logic (PCTL)/continuous stochastic logic (CSL), the tool enables the specification of complex measures, providing a nuanced understanding of system reliability and performance.
- Reward Event Trees with Embedded DFTs: SAFEST extends classical event trees by incorporating decision-making at states and embedding DFTs to provide transition probabilities. This allows for a detailed analysis of expected outcomes, frequency limits, and strategic decision-making to mitigate adverse effects.

4. Case study: safety system evaluation in a 10 MWth VVR reactor

4.1. Overview of the 10 MWth VVR reactor design

The design of the 10 MWth Vertical Volume Reactor (VVR) (F. Ameyaw et. al. 2021) is distinguished by its integration of five fundamental safety functions aimed at safeguarding the reactor core against damage following any initiating event. These safety functions encapsulate the core principles of nuclear safety: Reactivity Control, Core Cooling, Containment, Radiation Protection, and Emergency Response (Figure 2).

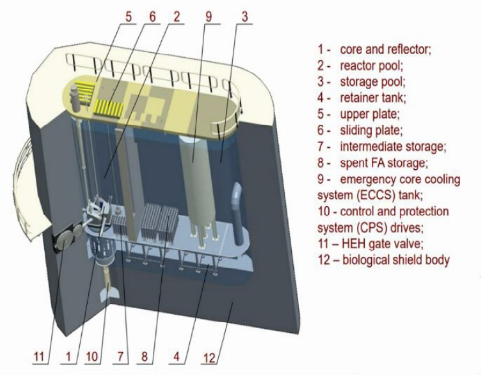


Fig. 2. Illustration of the different part of the reactor taken from (F. Ameyaw et. al. 2021).

Each function plays a pivotal role in the reactor's defence-in-depth strategy, ensuring operational safety under both normal and adverse conditions. Ensuring the utmost safety of the reactor operations, a multilayered safety system is implemented, comprising both passive and active components meticulously integrated to address a wide array of potential scenarios:

- Emergency Core Cooling System (ECCS);
- Containment Isolation System;
- Passive Cooling System.

A critical initiating event considered in this study is the Loss of Coolant Accident (LOCA), modeled using a dynamic event tree (DET) to simulate the reactor's response to a coolant loss scenario. The sequence of events was meticulously identified and modeled using the SAFEST software, providing a structured analysis of the potential sequences that could arise from such an incident.

4.2. Sequence of events following LOCA

The scenario begins with a hypothetical guillotine break of a 12-inch pipe connected to the reactor's lower part, triggering a series of safety responses:

1. Reactor Protection System (RPS) Activation: Immediately following the LOCA, the RPS is activated, and manual interventions are employed to shut down the reactor, effectively halting the fission chain reaction through a scram operation.
2. Pool Isolation: In the event of an RPS malfunction, butterfly valves are designed to close—either manually or automatically—shortly after the incident, isolating the pool from the system. Successful isolation ensures that the reactor core remains submerged in pool water, maintaining a crucial coolant supply.
3. Natural Circulation Heat Removal (NCHR): The availability of pool water initiates the opening of the flapper valve, enabling natural cooling of the core. This passive cooling mechanism is sufficient to prevent core damage, given the effective scram operation, marking sequence number 1 as successful.
4. Emergency Core Cooling System (ECCS) Activation: If natural circulation fails to initiate or if the reactor fails to shut down via the RPS, the ECCS comes into play, spraying water over the core to remove decay heat and prevent core damage.
5. Containment Isolation: In scenarios where ECCS is non-operational, measures to isolate the reactor building are crucial to prevent radioactive release into the environment. Effective containment isolation is supplemented by the emergency ventilation system, which releases pressure and filters out radioactivity.

This case study's in-depth analysis of the 10 MWth VVR reactor's response to a LOCA scenario underscores the significance of integrated safety functions and the dynamic interplay of passive and active safety systems. By leveraging advanced analytical tools like SAFEST and employing a structured approach to scenario modeling, the study highlights the effectiveness of the reactor's safety design in managing and mitigating critical initiating events, thereby ensuring the reactor's operational safety and the protection of the environment.

5. Results

The comprehensive analysis conducted on the 10 MWth VVR reactor, utilizing the SAFEST tool and incorporating dynamic modeling techniques, yielded insightful results into the reactor's safety systems' functionality and reliability during a hypothetical Loss of Coolant Accident (LOCA). Through the application of event tree analysis for LOCA scenarios (DET) and detailed modeling, we systematically evaluated the sequence of events, the role of safety systems, and their sequential activation to mitigate the LOCA impact.

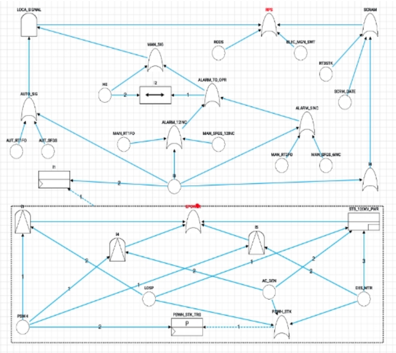


Fig. 3. Partial view of the DFT generated in this work by SAFEST tool.

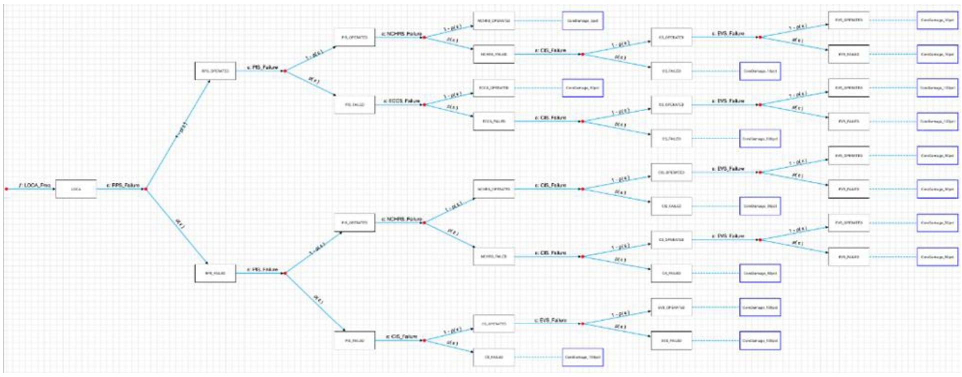


Fig. 4. The DET generated for this study.

5.1. Sequence analysis of safety system DFTs and DETs

Through the Dynamic Fault Tree (DFT) analysis of nuclear reactor safety systems, we gain an intricate understanding of how these systems interplay and potentially fail under stress, such as a Loss of Coolant Accident (LOCA). The analysis meticulously evaluates the Reactor Protection System (RPS) for its quick shutdown capability, the Pool Isolation (RPI) system for maintaining coolant levels, and the Natural Circulation Heat Removal (NCHR) system for its passive cooling efficiency. Additionally, it scrutinizes the Emergency Core Cooling System (ECCS) for backup cooling, the Containment Isolation System (CIS) for preventing radioactive releases, and the Emergency Ventilation System (EVS) for post-LOCA atmospheric control. This DFT-based evaluation not only highlights system vulnerabilities but also informs strategies for safety enhancement and maintenance prioritization, contributing significantly to the reactor's overall safety and operational reliability.

The LOCA Event Tree serves as a pivotal tool for interpreting the diverse pathways and potential outcomes following a coolant loss incident within a reactor, laying out a clear visual map of how safety systems sequentially respond to such an event. Starting with the initiating LOCA, the tree methodically branches out, showcasing the various decision points that determine the subsequent responses of the reactor's safety mechanisms.

At each branching point, probabilities derived from detailed Dynamic Fault Tree (DFT) analyses of each safety system come into play, offering a quantified likelihood of system performance under the stress of a LOCA. These probabilities are essential, as they illuminate the chances of either success or failure in each safety system's response, directly impacting the reactor's ability to mitigate the incident.

Visual cues in the form of color-coded status indicators on the graphical plots further enhance the interpretability of these complex system interactions. Green indicates operational status, while red signals failure, providing an immediate sense of each component's condition post-LOCA. The flow from one system's response to the next within the DFTs, and subsequently on the event tree, illustrates a dynamic progression of outcomes based on the operational integrity of safety systems.

By leveraging the SAFEST tool for generating and integrating DFTs with the event tree, a comprehensive risk profile of the reactor is constructed. This integration allows for a holistic analysis that not only assesses the reliability of individual safety systems but also how their collective responses shape the overall risk landscape following a LOCA.

5.2. LOCA Bowtie Analysis results

The Bowtie Analysis for a Loss of Coolant Accident (LOCA) scenario at a 10 MWth VVR reactor presents critical frequencies and expected losses based on an operational timeline of 20,000 time units, with an initiating event frequency quantified as 0.000251. This frequency sets the baseline for assessing the probabilities of various consequence scenarios and the expected losses stemming from those scenarios.

In the aftermath of a simulated Loss of Coolant Accident (LOCA) at the 10 MWth VVR reactor, the findings are synthesized into two distinct tabular representations of Table 1 and 2. These tables encapsulate the probabilistic outcomes derived from the integration of Dynamic Fault Trees (DFTs) and Event Trees (ETs) within the SAFEST tool framework.

The Table 1 enumerates the predicted frequencies of various core damage scenarios that were postulated in the event of a LOCA. These scenarios range from a 5 percent damage level, suggestive of minor core impairment, to a 100 percent damage level, indicative of a complete core meltdown. The frequencies are reflective of the inherent risk probabilities ascertained through our rigorous dynamic modeling processes and serve as a cornerstone for evaluating the resilience of the reactor's safety mechanisms.

Table 1. Predicted core damage frequencies.

Index	Consequence	Expected Frequency [min, max]
0	CoreDamage_5pct	0.000028201345832320914
1	CoreDamage_10pct	0.00005642372978283205
2	CoreDamage_30pct	0.00004552578043816359
3	CoreDamage_50pct	0.0001009549991174933
4	CoreDamage_100pct	0.00011075359386550847

Following the consequence probabilities, the Table 2, 'Expected Losses', delves into the projected impacts of the core damage levels on human safety, environmental integrity, and radiological release. The potential losses are quantified in terms of casualties, radionuclide release measured in million curies, and land contamination expressed in square miles. These metrics offer a quantitative perspective on the potential human and environmental cost associated with each core damage gradation, emphasizing the criticality of the reactor's safety functions in mitigating these risks.

Table 2. Expected losses.

Index	Losses	Expected Value [min, max]
0	CasualtiesBy5pcCD	0 Lives
1	RadionuclideBy5pcCD	0 Million Curies
2	ContaminatedLandBy5pcCD	0 Square Miles
3	CasualtiesBy10pcCD	0 Lives
4	RadionuclideBy10pcCD	0 Million Curies
5	ContaminatedLandBy10pcCD	0 Square Miles
6	CasualtiesBy30pcCD	0.00004552578043816359 Lives
7	RadionuclideBy30pcCD	0.00004552578043816359 Million Curies
8	ContaminatedLandBy30pcCD	0.0022762890219081796 Square Miles
9	CasualtiesBy50pcCD	0.0000547774995587467 Lives
10	RadionuclideBy50pcCD	0.000605732999470496 Million Curies
11	ContaminatedLandBy50pcCD	0.002019109998234987 Square Miles
12	CasualtiesBy100pcCD	0.005537679693275424 Lives
13	RadionuclideBy100pcCD	0.0208491486511907 Million Curies
14	ContaminatedLandBy100pcCD	0.11629127355878392 Square Miles

In assessing the risks to human life in the event of a core damage scenario at a nuclear reactor, as it shown in the Table 2 the analysis differentiates between lower and higher severity cases. For minor core damage scenarios—ranging from 5 to 10 percent – the data reveal no expected casualties, suggesting that the reactor's safety barriers and emergency response protocols are robust and effective in protecting personnel and the public. This lack of expected casualties in such scenarios speaks to the strength of preventive measures and the efficacy of rapid response systems in place. Conversely, as the extent of core damage escalates to higher levels, between 30 to 100 percent, there is a discernible rise in the potential for casualties. This trend is indicative of the escalated risk associated with more severe core damage incidents, underscoring the indispensable role of containment systems and the necessity for meticulous emergency response planning.

5.3. Analysis of core damage frequencies

Figure 5 presents a crucial aspect of the reactor's risk profile, illustrating the dynamic nature of risk associated with core damage following a LOCA. The Figure shows a graph illustrating how the expected frequency of core damage (CD) varies over time given a Loss of Coolant Accident (LOCA) for a 10 MWth VVR reactor. This graph is significant in understanding the time-dependent risk profile of the reactor in the event of a LOCA, which occurs with an annual frequency of 2.51E-04 (or 0.000251). The horizontal axis of the graph represents the time elapsed since the initiation of LOCA, measured in hours (timebound). The vertical axis quantifies the expected frequency of different levels of core damage, ranging from 5% to 100% CD. Each line on the graph corresponds to a specific level of core damage severity and its expected frequency over time.

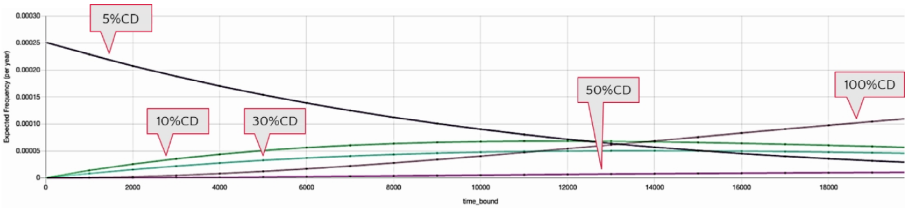


Fig. 5. Core Damage (CD) Expected frequency varies with LOCA occurrence time (hrs)- LOCA frequency/year: 2.51E-04.

The analysis of core damage frequencies following a Loss of Coolant Accident (LOCA) provides a nuanced understanding of the reactor's vulnerability over time. Initially, in the first 2000 hours post-LOCA, there's a notable predisposition towards minor levels of core damage (5% and 10% CD), suggesting immediate susceptibility to lesser damages following the incident. This initial vulnerability likely reflects the immediate aftermath of the LOCA, where the reactor's defenses are yet to fully mobilize or where the inherent resilience of the reactor is tested.

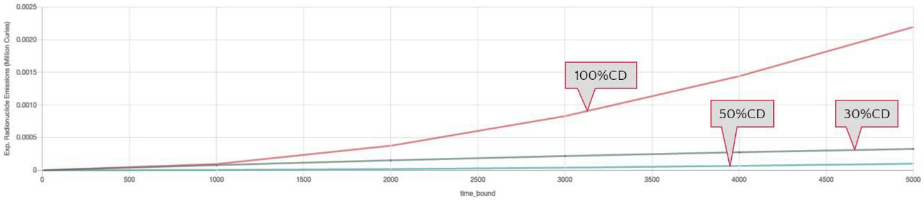
As one transitions into the mid-term phase, spanning from 2000 to 10000 hours, there's a discernible decrease in the expected frequencies for minor core damage. This decrease is indicative of the reactor's safety systems coming into effect, successfully mitigating further risk, or it could be attributed to the natural decay in heat production from the reactor core following its shutdown. This phase illustrates the efficacy of emergency protocols and safety systems designed to contain and minimize damage post-incident.

The long-term phase, extending beyond 10000 hours, unveils a concerning trend: an uptick in the expected frequency of more severe core damage levels (50% and 100% CD). This gradual increase signals a growing risk of substantial damage if initial LOCA impacts are not comprehensively addressed or if the reactor fails to stabilize from the initial event. The escalation suggests a cumulative effect of unmitigated damages or the inadequacy of long-term recovery strategies.

Most notably, the graph highlights peaks in severe core damage (50% and 100% CD) scenarios, pinpointing critical junctures where the reactor faces heightened risks of significant damage. These peaks underscore moments of acute vulnerability, possibly due to compounded damages or systemic failures in addressing the LOCA's consequences. Such insights are crucial for understanding the temporal dynamics of reactor safety post-LOCA, emphasizing the importance of robust, timely, and sustained response measures to safeguard the reactor's core integrity across all phases following a LOCA.

5.4. Analysis of contamination scenarios

Figure 5 illustrates how the expected area of contamination due to a Loss of Coolant Accident (LOCA) at a nuclear reactor change over time. Figure 5 is integral to understanding the environmental risks associated with a LOCA at different core damage levels over time. It demonstrates the need for timely containment and mitigation actions to minimize the spread of radioactive contamination. The horizontal axis of the graph represents the time elapsed since the initiation of a LOCA, measured in hours (time_bound). The vertical axis quantifies the expected contaminated area, likely measured in square miles or another appropriate unit of area. Each line on the graph correlates to the expected contaminated area corresponding to different core damage (CD) scenarios, from 30% CD to 100% CD.



The analysis of contamination scenarios depicted in the Figure 6 illustrates a comprehensive view of how the expected contaminated area evolves from the early phase post-LOCA through to the later stages, reflecting the effectiveness of containment strategies and their impact on environmental safety. In the initial hours following a LOCA (0-1000 hours), the graph indicates minimal contamination across all levels of core damage, pointing to the reactor's containment systems' efficacy in preventing the spread of radioactive materials. However, as the scenario unfolds into the mid-phase (1000-3000 hours), there's a marked increase in contamination, especially in instances of 100% core damage, signaling a heightened risk of environmental impact possibly due to containment failures or the buildup of radioactive substances.

Fig. 6. Expected contaminated area varies with LOCA occurrence time (hrs).

This trend of escalating contamination continues into the late phase (3000-5000 hours), particularly exacerbated in the most severe damage scenarios. Such observations underscore the critical nature of timely and effective containment and mitigation measures to curb the environmental repercussions of a LOCA. The graph's slopes for each core damage scenario serve as indicators of the contamination risk's growth rate over time, with steeper inclines for more significant damage levels highlighting the urgent need for proactive containment strategies.

The difference in slopes between the 30%, 50%, and 100% CD lines indicates that the severity of the core damage has a direct correlation with the rate of radionuclide emissions. Higher severity leads to more significant and faster increases in emissions. The steep rise in the 100% CD scenario underscores the critical need for effective early response to LOCA incidents. Delayed or inadequate response could result in scenarios where radionuclide emissions increase drastically, posing severe health and environmental risks. These results emphasize the importance of maintaining the integrity of containment systems and having robust mitigation strategies in place to manage and contain radionuclide emissions effectively, particularly in the hours and days following a LOCA. Figure 6 provides essential insights into the temporal dynamics of radionuclide emissions following a LOCA at a nuclear reactor. Understanding these dynamics is vital for emergency preparedness and response planning, ensuring that measures to protect human health and the environment are in place and can be effectively activated in the event of a nuclear incident.

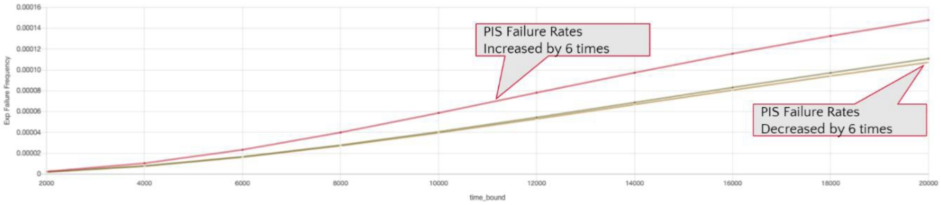


Fig. 6. Sensitivity analysis: 100% core damage (CD) expected frequency depends on failure rates of pool isolation system (PIS).

5.5. Sensitivity analysis

The Figure 7 illustrate how changes in the failure rates of the Pool Isolation System (PIS) affect the expected frequency of a 100% core damage scenario following a Loss of Coolant Accident (LOCA) in a nuclear reactor. The horizontal axis indicates the time elapsed since a LOCA, measured in hours (timebound). The vertical axis measures the expected frequency of 100% core damage occurring. Two curves represent scenarios where the failure rates of the PIS have either increased by six times or decreased by six times.

The steeper curve illustrates that when the failure rates of the PIS are increased by a factor of six, the probability of experiencing a complete core damage rises significantly over time. This suggests that the PIS is a critical component in the reactor's safety system, and its reliability strongly influences the overall risk profile of the reactor in the event of a LOCA. Conversely, the shallower curve shows that when the PIS failure rates are decreased by a factor of six, the expected frequency of 100% core damage is considerably lower. This indicates that enhancing the reliability of the PIS can effectively reduce the risk of severe core damage.

The graph demonstrates the importance of the PIS in maintaining reactor safety. A reliable PIS contributes significantly to lowering the probability of catastrophic core damage scenarios. The sensitivity analysis highlights the need to prioritize maintenance efforts for the PIS and possibly to redesign the system for greater resilience, given its high impact on reactor safety.

6. Conclusion

Drawing upon the intricate methodologies applied and the data garnered from the SAFEST tool, this study has culminated in a profound understanding of the safety dynamics within a 10 MWth VVR reactor experiencing a Loss of Coolant Accident (LOCA). The integration of dynamic fault trees (DFTs), event trees (ETs), and sophisticated sensitivity analyses has provided a granular view of the reactor’s risk profile, marrying the theoretical rigor of probabilistic risk assessment with practical insights into reactor safety management.

Our approach employed advanced modeling techniques to construct DFTs and ETs that reflect the intricate network of dependencies and potential failure modes within the reactor's safety systems. The quantitative evaluation of these models illuminated the probabilistic nature of various core damage scenarios, shedding light on the efficacy of safety systems under different operational conditions. By simulating a range of LOCA scenarios and analyzing the resultant data, we established a spectrum of risk probabilities for core damage and subsequent radiological impacts.

A novel aspect of this study was the sensitivity analysis of the Pool Isolation System (PIS), which revealed its critical role in the reactor's overall safety posture. By systematically adjusting the PIS failure rates, we assessed how variations in system reliability could affect the likelihood of severe core damage. This sensitivity analysis not only demonstrated the importance of robust system components but also highlighted the utility of proactive safety system management and the potential benefits of design modifications aimed at enhancing system resilience.

The reported frequencies for minor core damage scenarios (5-30%) confirmed the reactor's design robustness and the operational efficiency of its safety systems. The absence of expected casualties in these scenarios reflects well on the safety barriers and emergency protocols in place. For higher damage levels (50-100%), although the probabilities increased, the findings prompted a reevaluation of containment and emergency response strategies to mitigate the risks associated with more severe damage outcomes.

In conclusion, the multifaceted analysis conducted in this study represents a significant contribution to the field of nuclear safety. By leveraging the capabilities of the SAFEST tool to its full potential, we have delineated a path forward that not only enhances our understanding of the risks inherent in nuclear reactor operations but also paves the way for the development of more resilient safety strategies. This comprehensive approach to probabilistic safety analysis embodies the cutting edge of nuclear risk assessment and offers a replicable model for future studies aiming to marry precision in probabilistic modeling with the practical exigencies of nuclear safety and operational planning.

Acknowledgements

We extend our deepest gratitude to ASSYSTEM and DGB Technologies for providing the necessary resources to support this research.

References

Ajmone-Marsan, M., G. Balbo, G., Conte, S., Donatelli, G., Franceschinis, 1995. Modelling with Generalized Stochastic Petri Nets. Wiley Series in Parallel Computing.

Ameyaw, F., Abrefah, R., Yamoah, S., Birikorang, S. 2021. Analysis and Estimation of Core Damage Frequency of Flow Blockage and Loss of Coolant Accident: A Case Study of a 10 MW Water-Water Research Reactor-PSA Level 1, Science and Technology of Nuclear Installations, Article ID 9423176, 17 pages.

Baek, S., Heo, G. 2021. Application of Dynamic Fault Tree Analysis to Prioritize Electric Power Systems in Nuclear Power Plants. Energies 14. 4119. 10.3390/en14144119.

Baoping, C., 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. doi:10.1016/j.ress.2021.107464.

Dugan, J.B. 1993. Fault Trees and Markov Models for Reliability Analysis of Fault-Tolerant Digital Systems. Reliability Engineering & System Safety 39, no. 3.

IAEA TEC DOC-1474, 2005. Natural Circulation in Water Cooled Nuclear Power Plants. Phenomena, models, and methodology for system reliability assessments, November 2005.

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

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

Jafari, J., D’Auria, F., Kazeminejad, H., Davilu, H. 2003. Reliability evaluation of natural circulation system. Nucl. Eng. Des. 224, 79-104.

Kabir, S., Papadopoulos, Y. 2019. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review. Safety Science 115, 154-175.

Khare, V., Nema, S., Baredar, P. 2018. Reliability analysis of hybrid renewable energy system by fault tree analysis. Energy & Environment 30.

Marquès, M., Pignatel, J., Saignes, P., D’Auria, F., Burgazzi, L., Müller, C., Bolado-Lavin, R., Kirchsteiger, C., La Lumia, V., Ivanov, I. 2005. Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment. Nucl. Eng. Des. 235, 2612–2631.

Verma, A.K., Ajit, S., Kumar, S. 2022. Dynamic Fault Tree Analysis for Nuclear Reactor Safety Assessment. Nuclear Engineering and Technology 54(5), 1503-1512.

Volk, M., Sher, F., Katoen, J.-P., Stoelinga, M. 2024. SAFEST: Fault Tree Analysis Via Probabilistic Model Checking. Annual Reliability and Maintainability Symposium (RAMS), Albuquerque, NM, USA, 1-7.

Zhang, Y., Mosleh, A. 2020. Methodologies in Probabilistic Safety Assessment for Nuclear Power Plants. Progress in Nuclear Energy 118, 103162.