Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P7685-cd

Dynamic reliability and safety modeling of a molten salt reactor using SysML v2

Luigui Salazar

Technology & Innovation, ASSYSTEM, Paris, France. E-mail: lasalazarcabrer@assystem.com

Masood Akmali

Innovation Digital BU, ASSYSTEM, Paris, France. E-mail: makmali@assystem.com

Falak Sher

DGB Technologies Duisburg, Germany. E-mail: chfalak@dgbtek.com

Ahmad Zafar

DGB Technologies Duisburg, Germany. E-mail: ahmad.zafar@dgbtek.com

Robert Plana

Technology & Innovation, ASSYSTEM, Paris, France. E-mail: lasalazarcabrer@assystem.com

The increasing demand for clean and sustainable energy sources has reignited interest in nuclear power, with Molten Salt Reactors (MSRs) emerging as a promising innovation due to their enhanced safety, efficiency, and sustainability compared to traditional solid-fuel reactors. However, the large-scale deployment of MSRs faces critical challenges, particularly the corrosive nature of molten salts and the complex interdependencies of system components, which necessitate advanced methods for safety and reliability assessment. This study pioneers a model-based safety and reliability assessment of an MSR system using the Systems Modeling Language (SysML) v2. This approach facilitates a holistic and system-engineering-driven representation of the MSR, encompassing requirements, constraints, metadata, and system architecture. The focus is on the primary fuel loop, specifically the primary heat exchanger and fuel pump, two key subsystems that are critical for efficient reactor operation. The SysML v2 model, annotated with safety information, is consumed by the SAFEST toolchain, a state-of-the-art probabilistic risk assessment (PRA) platform, generating safety artifacts – dynamic fault trees – and evaluating metrics like unreliability, full functional availability (FFA), mean time to failure (MTTF), etc. This methodology automates the generation of safety artifacts from SysML v2 models of dynamic systems, capturing time-dependent failure behavior and fault propagation pathways that static approaches cannot fully address. This study represents the first application of dynamic reliability artifact generation, which captures the time-dependent failure behavior of MSR system components, to an MSR system modeled in SysML v2, setting a new benchmark for model-based safety assessments in complex nuclear systems. The results provide quantitative insights into system reliability metrics, identify critical failure-prone components, and highlight opportunities for design refinement and optimization. This systematic approach provides a scalable framework for evaluating the safety and reliability of MSR and other complex engineered systems, contributing to their viability as a sustainable energy solution for the future.

Keywords: SysML v2, molten salt reactor, nuclear energy, dynamic fault trees, reliability assessment

1. Introduction

The pursuit of clean and sustainable energy sources has become an increasingly pressing concern in recent years, driven by growing concerns over climate change, air pollution, and energy security (Batteux, M 2022). In this context, nuclear power has emerged as a promising alternative to fossil fuels, offering a low-carbon source of electricity that can help mitigate these challenges. However, the history of nuclear power is marked by significant safety incidents, such as

the Fukushima Daiichi accident in 2011 (Kondratyk V 2023), which have highlighted the need for enhanced safety and efficiency measures.

Reliability analysis of complex systems like MSRs requires a comprehensive and structured approach that goes beyond traditional document-based methods (Dugan, J.B. (1993). The increase in system complexity has led to the emergence of Model-Based Systems Engineering (MBSE), which replaces static document-centric approaches with formal, dynamic models that offer a holistic view of system structure, behavior, and interdependencies (Batteux, M et al. 2022). Through MBSE, system designers and reliability engineers can collaboratively develop, simulate, and validate system models, ensuring early detection and resolution of design flaws and inconsistencies (Creff, S. & Batteux, M. 2022).

Modern engineered systems are becoming increasingly complex due to their multi-functional, multi-domain nature. Addressing the complexities associated with these interdependencies requires a modeling approach that can capture both the structural and behavioral aspects of the system. Traditional analysis methods based on static system representations fall short in this regard, as they cannot accurately capture failure dependencies or time-dependent interactions. System modeling is essential for supporting the early-stage design of complex systems (M. Akmali et al. 2023). By employing system models, engineers can simulate different design alternatives, explore potential failure modes, and assess system behavior in response to varying conditions (Rauzy, A. 2022). Importantly, system modeling facilitates the generation of probabilistic risk assessments (PRA), which are crucial for quantifying the likelihood of system failures and for ensuring compliance with safety standards.

To model, analyze, and verify complex systems, engineers require a unified modeling language that can accurately represent system architecture, requirements, constraints, and design logic. The Systems Modeling Language (SysML) has emerged as a standard language for MBSE. SysML enables the development of system models that encompass not only structural representations but also behavioral interactions and operational scenarios (Biggs, G. et al. 2016 & Munk, P. & Nordmann, A. 2020). Unlike traditional UML (Unified Modeling Language), which is primarily used for software systems, SysML is tailored to support multi-disciplinary engineering involving mechanical, electrical, and software domains. Traditionally system engineers and safety experts work together to verify safety requirements of systems at design time. Safety experts understand system models from engineers, and then manually generate safety artifacts as per the safety requirements. This process is quite time consuming as after each iteration in the system design, the whole process of safety artifacts generation is repeated. Automating this process will not only decrease the design time but will also avoid manual errors.

Unlike SysML v1, its latest version, SysML v2, provides textual representation of system models, thus providing single point of truth for all kinds of system behaviors. This opens doors of automatic mode-based safety assessment (MBSA) in parallel to system-based model-engineering (MBSE) so that unlike traditional system descriptions that focus on static structures, SysML v2 allows dynamic fault trees (DFTs) to be incorporated into the system model. This is a major advancement, as DFTs allow for the representation of time-dependent failure behaviors, component interactions, and cascading effects. For instance, the failure of a fuel pump in an MSR may trigger a chain of failures in other interconnected components, and such interdependencies can be explicitly modeled in SysML v2.

In this study, we present a comprehensive model-based approach for safety and reliability assessment of an MSR system, focusing on the

primary fuel loop. The primary fuel loop, which includes the primary heat exchanger and fuel pump, is crucial for heat transfer and fuel circulation. We employ SysML v2 to capture the system structure, functional requirements, and behavioral dynamics of this subsystem. We annotate safety related information, e.g. redundancy among pumps, etc., in the SysML v2 model. By importing this model into the SAFEST toolchain (Volk M 2024 & Akmali et al. 2024), we automatically generate dynamic fault trees and compute some sample measures such as Unreliability probability, Mean Time to Failure (MTTF) and Full Functional Availability. Due to space constraints, we only computed a few measures as given by Majdi Ghadhab et al. 2019.

By utilizing Jupyter Lab as an integrated development environment (IDE) for edition and visualization and SAFEST for computational analysis, we achieve a dynamic and quantitative assessment of system reliability. Therefore, the current paper is organized as follows. After the introduction Section 2 reminds the Model Based Safety and Reliability assessment Analysis. In Section 3, the SAFEST tool chain is presented to demonstrate the benefits of the tools. After explaining the methodology in section 4, the case study is briefed in Section 5. The results and discussions are outlined in sections 6 and 7 respectively. Finally, the concluding remarks are outlined in section 8.

2. Model-Based Safety and Reliability Assessment

Reliability assessment is an essential aspect of MSR system design due to the high-risk nature of nuclear energy systems (Boussier, H 2012). Traditional approaches to system reliability often rely on static, document-based methods, but these methods are insufficient for capturing the dynamic nature of system failures. Model-Based Safety Assessment (MBSA), a subset of MBSE, addresses this challenge by creating integrated models of system design and safety analysis. By employing SysML v2 for MBSA, the system architecture and safety models are automatically synchronized, reducing the likelihood of inconsistencies. This synchronization ensures that the fault models and safety artifacts remain aligned with system changes throughout the design lifecycle.

The SAFEST toolchain facilitates the automatic generation of safety artifacts, Fault Tree Analysis (FTA), and Dynamic Fault Tree Analysis (DFTA), allowing for the efficient quantification of system safety metrics. The contributions of the current study are threefold:

1. **First-of-its-kind Dynamic Reliability Analysis:** This work represents the first application of SysML v2 for generating dynamic reliability artifacts for an MSR system. By employing SysML v2 and the SAFEST toolchain, we can generate dynamic failure metrics that account for time-dependent failure behaviors and cascading failures.
2. **Comprehensive Model-Based Assessment**: We present a model-based safety and reliability assessment of the primary fuel loop of an MSR system. This analysis includes the dynamic reliability assessment in terms of the time-dependent failure behavior of the primary heat exchanger and the fuel pump, which are critical subsystems for the safe operation of the reactor.
3. **Advanced System Description and Traceability**: By adopting SysML v2, we provide a comprehensive description of system structure, constraints, and behavioral interdependencies. The ability to generate and synchronize safety artifacts ensures full traceability and alignment between system design and safety models, thus supporting continuous improvement and optimization of the system design.

3. SAFEST Toolchain for Dynamic Reliability Assessment

The SAFEST toolchain is a cutting-edge software platform designed for dynamic reliability and safety assessment of complex systems, such as Molten Salt Reactors (MSRs). Unlike traditional static reliability analysis methods, SAFEST leverages Dynamic Fault Trees (DFTs) to model time-dependent failures, functional dependencies, and spare management.

One of the most significant features of SAFEST is its integration with SysML v2, which allows system models to be directly imported and converted into Dynamic Fault Trees (DFTs). This integration ensures model consistency throughout the system's lifecycle, aligning system design with safety analysis. The tool also analyzes dynamic fault trees through supporting state-space generation via, probabilistic model checking, and dynamic event tree (DET) analysis, enabling the quantification of key rich set of reliability metrics. The SAFEST toolchain is equipped with an interactive, web-based interface that features drag-and-drop fault tree editors, empirical distribution support, and graphical visualization of reliability metrics. It offers both static and dynamic analysis capabilities by combining Binary Decision Diagrams (BDDs) for static components and Markov Automata (MA) for dynamic behavior. This hybrid analysis approach reduces computational complexity and ensures scalability for large, multi-component systems.

In this study, the SAFEST toolchain was used to analyze a simplified model of the MSR system, focusing on key subsystems like the primary heat exchanger and the fuel pump. The analysis revealed critical fault propagation pathways and generated dynamic reliability artifacts such as MTTF, FFA, and system availability over time.

4. Methodology

This study employs a Model-Based Safety and Reliability Assessment approach, integrating SysML v2 for system modeling with SAFEST for dynamic reliability analysis. The process ensures consistency from system design to reliability assessment, focusing on the primary fuel loop of the Molten Salt Reactor (MSR), particularly the primary heat exchanger and fuel pump subsystems. The methodology follows four principal steps:

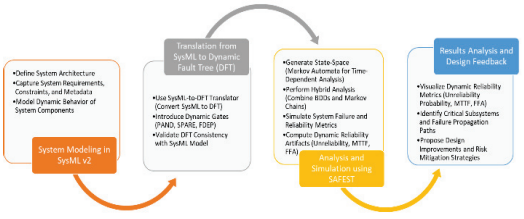

Fig 1. The general methodology adopted in this study.

i. **System Modeling Using SysML v2:** The process begins with the development of a comprehensive system model using SysML v2. This model captures the architecture, behavior, and interdependencies of system components. The primary fuel loop is modeled to include subsystems like the primary heat exchanger and fuel pump, incorporating requirements, constraints, and operational metadata. Behavioral models are developed to represent failure propagation and dynamic interactions among system components. The model components are annotated, using metadata construct of SysML v2, with safety related information e.g. which two pumps are redundant to each other, whether it is a cold redundancy, hot or warm, etc.

ii. **Translation from SysML v2 to Dynamic Fault Tree (DFT)**: The SysML v2 model is exported to a Dynamic Fault Tree (DFT) using the SysML-to-DFT translator. This step captures system structure, component behavior, and fault interdependencies. Dynamic gates like Priority AND

(PAND), SPARE, and Functional Dependency (FDEP) are used to model sequential and functional dependencies between failures. The DFT is validated to ensure alignment with the original SysML model.

iii. **Dynamic Reliability Analysis Using SAFEST**: The SAFEST tool is used to analyze the DFT, focusing on dynamic system behavior. The analysis begins with state-space generation of dynamic sub-trees using Markov Automata (MA) via probabilistic model-checking to represent component states. A hybrid analysis is conducted, using Binary Decision Diagrams (BDDs) for static components and Markov Chains for dynamic elements. This step captures failure propagation paths, revealing how failures in components like the fuel pump affect other subsystems.

iv. **Results Analysis and Feedback**: The results from SAFEST are analyzed to identify critical components and failure pathways. Key insights are visualized through interactive reliability graphs, showing how different metrics evolve over time. Through an iterative feedback loop continuous improvement in system design and safety can be ensured.

5. Case Study: Molten Salt Reactor (MSR)

The Molten Salt Reactor (MSR) is a next-generation nuclear reactor with significant potential for safety, efficiency and sustainability. Unlike traditional solid-fuel reactors, MSRs use molten salt as both fuel and coolant, allowing for continuous fuel circulation. This unique design offers several advantages, including inherent passive safety, low operating pressure, and efficient heat transfer. Despite these advantages, MSRs introduce new engineering challenges related to high-temperature operations, corrosive environments, and thermal-hydraulic behavior, all of which must be carefully managed through advanced modeling, simulation, and reliability analysis.

This study applies a Model-Based Safety and Reliability Assessment (MBSA) approach to the primary fuel loop of the MSR, focusing on key subsystems such as the primary heat exchanger and fuel pump. Using SysML v2 for system modeling and the SAFEST toolchain for reliability analysis, a comprehensive view of system reliability is obtained. The analysis includes the identification of critical components, interdependencies, and system failure pathways, providing actionable insights for improving system design and safety.

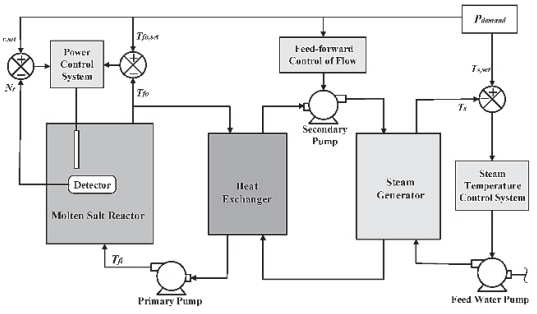

Fig 2. a simplified model of an MSR.

Figure 2 illustrates a simplified model of a MSR. The primary fuel loop of the MSR plays a pivotal role in energy transfer and heat management. It circulates the molten salt fuel (typically LiF-ThF4-UF4) from the reactor core to the heat exchanger, where thermal energy is transferred to a secondary coolant.

The primary circuit begins with the flow of molten salt fuel from the reactor core to the fuel pump, which ensures continuous fuel flow. The fuel is transported to the primary heat exchanger, where it releases thermal energy to a secondary coolant (typically CO_2). The following are the key components of the primary circuit:

- **Fuel Pump**: Maintains the continuous flow of molten salt through the system, ensuring proper fuel circulation and supporting heat transfer in the heat exchanger.

- **Heat Exchanger**: Facilitates the transfer of thermal energy from the molten salt to the coolant through a plate-type design.
- **Off-Gas System**: Manages the removal of gaseous fission products and particulates from the fuel salt, improving overall reactor performance and mitigating potential failure risks.

A system failure model is developed to identify failure dependencies and failure propagation pathways within the MSR system. Each critical subsystem is modeled using a combination of AND/OR gates and dynamic fault gates (PAND, SPARE) to capture time-dependent failures. The exponential failure distribution is applied to each component, allowing for the calculation of system failure probabilities and system reliability (IAEA 1998).

The model is exported from SysML v2 to SAFEST in JSON format, enabling dynamic reliability analysis (DGB Technologies. 2020).

6. Results

This section presents and interprets the results obtained from the dynamic fault tree analysis (DFTA) of the Molten Salt Reactor (MSR) system. Using the failure rates extracted from the IAEA reliability database and expert advice, the analysis provides the Mean Time to Failure (MTTF), unreliability probability, and Full Functional Availability (FFA) over a 1000-hour operational period.

6.1 *Dynamic fault trees generation and reliability assessment*

The dynamic fault tree shown in Figure 3 is generated based on the SysML v2 model of the MSR, representing the fault propagation pathways and interdependencies among critical components, capturing both static and dynamic failures, including sequential dependencies and functional relationships (e.g., AND/OR gates).

The primary focus of the fault tree is on the primary fuel loop, particularly the fuel pump system, heat exchanger, and secondary coolant management.

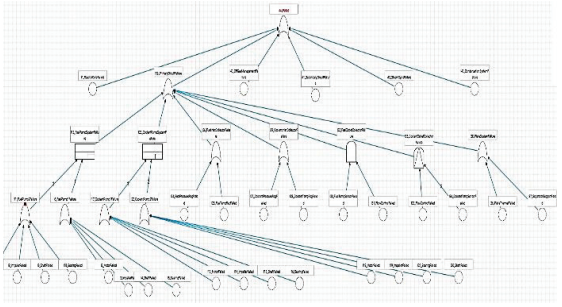

Fig 3. Dynamic Fault Tree generated in this study.

6.2 *Mean Time to Failure (MTTF)*

The MTTF for the MSR system, as shown in Table 1, is derived accordingly as approximately 5047 hours. This value represents the expected operational time before the system encounters a critical failure.

The relatively high MTTF indicates that the MSR system, with its redundancy and failure mitigation strategies, is capable of sustained operation under normal conditions.

Table 1. Mean Time to Failure of the system.

Metric	Result (hr)
MTTF	5047.16

However, the fuel pump system contributes significantly to the overall failure probability, particularly due to components like the shaft seals and drive motor, which exhibit higher failure rates.

6.3 *Unreliability Probability*

As can be seen from Figure 4, the unreliability probability curve shows a gradual increase over time, reaching approximately 0.14 at 1000 hours of operation.

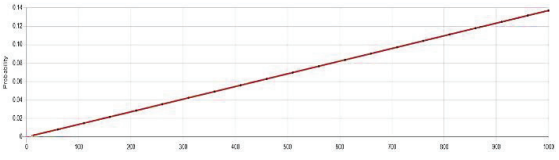

Fig 4. Unreliability probability of the system.

The linear trend of the curve reflects the use of exponential failure distributions, where failure rates remain constant over time.

The increase in unreliability is primarily driven by high-risk components such as the fuel pump bearings, shaft seals, and heat exchanger plates, which have relatively higher failure rates.

This result highlights the importance of regular maintenance and inspection of critical components to mitigate failure risks over extended operational periods.

6.4 *Full Functional Availability (FFA)*

The Full Functional Availability (FFA probability curve) depicted in Figure 5 shows a steady decline over time, dropping to approximately 0.65 after 1000 hours. The FFA represents the probability that the system remains fully operational without degradation.

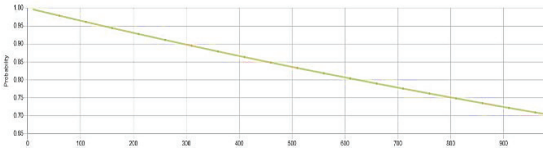

Fig 5. Full Functional Availability of the system.

In this analysis, system degradation is defined as the failure of both primary fuel pumps, requiring the secondary pumps to take over. This reflects a degraded operational state rather than a complete failure.

The gradual decline in FFA emphasizes the system's reliance on redundancy (e.g., secondary pumps) to maintain functionality under partial failure conditions.

7. Discussion

The analysis identifies fuel pump components (e.g., shaft seals, drive motor) and heat exchanger plates as major contributors to system unreliability. The results suggest that while redundancy improves system resilience, failures in primary components significantly reduce the availability of the system. Ensuring the reliability of critical components like pumps and heat exchangers is essential for maintaining high availability. These components require targeted design improvements, such as enhanced materials to resist corrosion and creep at high operating temperatures and improved redundancy mechanisms to reduce the impact of component failures.

The role of secondary pumps in maintaining system operation under degraded conditions highlights the importance of redundancy. However, the degradation in availability (FFA) suggests that improvements in primary pump reliability would significantly enhance system performance.

Given the relatively high unreliability at 1000 hours, predictive maintenance strategies should be implemented to monitor and replace high-risk components before failure occurs. This is particularly important for components with higher failure rates (e.g., shaft seals, impellers).

The results emphasize the need for optimization of the primary fuel loop design, with a focus on reducing failure probabilities in critical subsystems. This can be achieved through:

- Advanced materials and coatings for heat exchanger components.
- Improved seals and bearings for fuel pumps to extend their operational lifespan.

8. Conclusions

This study presents a comprehensive Model-Based Safety and Reliability Assessment of a Molten Salt Reactor (MSR) system, focusing on the primary fuel loop. By integrating SysML v2 for system modeling with the SAFEST toolchain for dynamic reliability analysis to capture the time-dependent accident sequences of the MSR system components, the methodology successfully identifies critical components, failure pathways, and key reliability metrics.

Using failure rates derived from the IAEA reliability database and expert advice, the analysis produced the following key insights:

- Mean Time to Failure (MTTF) of 5047 hours, indicating robust system performance under nominal conditions.
- Unreliability Probability reaches 0.14 after 1000 hours of operation, highlighting the gradual increase in

failure likelihood due to components with higher failure rates.

- Full Functional Availability (FFA) drops to approximately 0.65 at 1000 hours, underscoring the system's reliance on redundancy, particularly the secondary pumps, to maintain operation under degraded conditions.

The analysis identified fuel pump components (e.g., shaft seals, drive motors, and bearings) and heat exchanger plates as the most failure-prone elements. These components contribute significantly to the overall system unreliability and availability degradation.

This study demonstrates the effectiveness of combining SysML v2 and the SAFEST toolchain to perform dynamic reliability assessments of complex systems. The systematic approach ensures traceability, consistency, and the generation of reliable safety artifacts to inform design improvements. The findings contribute to ongoing research and development efforts aimed at ensuring the safety, reliability, and long-term viability of MSRs as a promising solution for clean and sustainable energy production.

Future work will focus on extending this methodology to other reactor components, incorporating additional failure modes, and integrating multi-physics simulations to further enhance system analysis. Moreover, all complex measures in Majdi Ghadhab (2019) will be evaluated for the whole system.

References

Batteux, M., Choley, J.-Y., Mhenni, F., Prosvirnova, T., & Rauzy, A. (2022). Synchronization of system architecture and safety models: a proof of concept.

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

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.

Creff, S., & Batteux, M. (2022). Characterizing behavioral modeling in systems and safety model-based engineerings and their overlap for consistency checking.

Majdi Ghadhab, Sebastian Junges, Joost-Pieter Katoen, Matthias Kuntz, Matthias Volk, (2019). Safety Analysis for Vehicle Guidance Systems with Dynamic Fault Trees, Reliability Engineering and System Safety.

Legendre, A., Druet, J., Serru, T., Laguilliez, R., & Donat, R. (2020). Interest of the K6 2.0 tool for the RAMS analysis of critical electrical networks.

Biggs, G., Sakamoto, T., & Kotoku, T. (2016). A profile and tool for modelling safety information with design information in SysML. Software & Systems Modeling, 15(1), 147–178.

Munk, P., & Nordmann, A. (2020). Model-based safety assessment with SysML and component fault trees: application and lessons learned.

Rauzy, A. (2022). Model-based reliability engineering: An introduction from first principles.

Boussier, H., S. Delpech, V. Ghetta, D. Heuer, D-E. Holcomb, V. Ignatiev, E. Merle-Lucotte, and J. Serp, (2012). "The molten salt reactor (MSR) in Genration IV: overview ans perspectives." In 2nd Generation IV International Forum (GIF) Symposium, pp. 95-107.

M. Akmali, R. Plana, and F. Sher. (2024). Evolving PSA Methodologies: Towards Dynamic Reliability in SMR Passive Systems. IAEA Conference

DGB Technologies, (2020). SAFEST features overview and capabilities report,

INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), (1998). component reliability data for use in probabilistic safety assessment. IAEA-TECDOC-478.

Nagy, K., D. Lathouwers, C. G. A. T'Joen, J. L. Kloosterman, and T. H. J. J. Van Der Hagen, (2014). "Steady-state and dynamic behavior of a moderated molten salt reactor." Annals of Nuclear Energy 64 365-379.

Zhuang, Kun, Liangzhi Cao, Youqi Zheng, and Hongchun Wu, (2015). "Studies on the molten salt reactor: code development and neutronics analysis of MSRE-type design." Journal of Nuclear Science and Technology 52, no. 2: 251-263.

Tiberga, Marco, (2020). "Development of a high-fidelity multi-physics simulation tool for liquid-fuel fast nuclear reactors." PhD diss., Delft University of Technology.

V., Kondratyk., Y., M., Pysmennyy., I.O., Ostapenko., D., K., Fedorov. (2023). 3. Accident lessons at the fukushima-daiichi npp for the safety of the nuclear power industry in ukraine. Energetika. Ekonomìka, tehnologiï, ekologiâ,