Human Systems Engineering and Design (IHSED 2026), Vol. 237, 2026, 757–766
https://doi.org/10.54941/ahfe1008214

Dynamic Requirement Verification and Safety Assessment of Complex Systems Using MBSE and Co-Simulation

Sandra Gyasi, Mouna El Alaoui, Nicolas Bureau, Robert Plana, and Camilo Murillo Coba

Digital Excellence Centre, Assystem Energy and Operation, Courbevoie, France

ABSTRACT

Critical infrastructures, particularly nuclear energy systems, face growing complexity due to regulatory constraints, performance demands, and the transition toward low-carbon power. Model-Based Systems Engineering (MBSE) supports complexity management by linking system architecture with multiphysics simulation, ensuring traceability from requirements to behavior. However, most MBSE verification approaches remain limited to nominal operating conditions and do not explicitly integrate reliability-driven degradation into requirement evaluation. In practice, aging, wear-out mechanisms, and random faults progressively erode safety margins, limiting early detection of degraded performance. This paper proposes an integrated methodology combining MBSE with stochastic degradation modeling for dynamic requirement verification under both functional and degraded scenarios. A stochastic Petri net (SPN) with Weibull-distributed transitions is embedded into a Dymola physical model to represent time-dependent failure behavior. Safety and performance requirements are formalized using the Common Requirement Modeling Language (CRML) within a SysML architecture model developed in Catia Magic and continuously evaluated during co-simulation. Interoperability between architectural and behavioral domains is ensured via Functional Mock-up Units (FMUs) and UDP-based communication, preserving synchronization and bidirectional traceability. The framework is applied to the primary loop of a Molten Salt Reactor (MSR), focusing on stochastic degradation of the primary fuel pump over 5000 s simulation. Results show a 39% mass-flow reduction, core temperature rise beyond the 708 °C safety limit, and an 18% increase in thermal power, demonstrating significant safety margin erosion. The proposed approach transforms verification from static compliance checking into a dynamic, reliability-aware assessment of system behavior over time.

Keywords: MBSE, Complex systems, Physical modelling, Co-simulation, Common requirement modeling language, MSR

INTRODUCTION

Modern cyber-physical systems (CPS), such as advanced nuclear reactors, involve tightly coupled multidisciplinary components and complex safety requirements (Topper and Horner, 2013). Ensuring compliance with safety and performance constraints throughout the system lifecycle remains a major challenge. Model-Based Systems Engineering (MBSE) addresses

Received April 17, 2026 Revised June 19, 2026 Accepted July 1, 2026 Available online September 25, 2026

this complexity by integrating system architecture models with executable simulations, improving traceability, consistency, and early validation (Kaslow et al., 2014).

Formal requirement modeling enhances MBSE by enabling executable verification of temporal and logical constraints. The Common Requirement Modeling Language (CRML) defines requirements as spatiotemporal constraints evaluated during co-simulation (Bouskela et al., 2023), while approaches such as FORM-L extend simulation environments for time-dependent verification (Bouskela et al., 2022). Combined with interoperability standards like the Functional Mock-up Interface (FMI) (Modelica Association, 2014), these methods enable real-time coupling between system architecture and physics-based simulation tools.

However, most MBSE-based verification approaches focus on nominal operating conditions. In practice, components degrade due to aging and random faults. Reliability engineering shows that wear-out phenomena, modeled using Weibull distributions ($\beta>1$), lead to increasing failure rates over time (Montgomery and Runger, 2018). Stochastic Petri Nets (SPNs) provide an effective framework to represent probabilistic and time-dependent degradation (Kleyner and Volovoi, 2010), and have been applied to model degradation of critical MSR components (Gyasi and Akmali, 2025).

Despite these advances, MBSE, reliability modeling, and requirement verification are often treated separately. This limits traceability and delays feedback, particularly in safety-critical systems where degradation can affect performance and safety margins.

To address this gap, this work proposes an integrated framework combining MBSE, multiphysics simulation, stochastic degradation modeling, and executable requirement verification within a real-time co-simulation environment. A SysML-based architecture is coupled with a Dymola model incorporating CRML requirements and an SPN-based reliability model. This enables continuous and traceable verification under both nominal and degraded conditions.

The contributions include a unified co-simulation framework, integration of stochastic degradation into requirement verification, real-time synchronization between tools using FMI, and demonstration on an MSR case study highlighting degradation impacts on safety margins.

METHODOLOGY

Figure 1 illustrates the integrated methodology adopted in this study. The framework extends the Digital Safety approach by combining Model-Based Systems Engineering (MBSE), physical simulation, and stochastic degradation modeling within a unified digital environment. This integration enables consistent verification and validation of safety and performance requirements for complex systems, from conceptual design to operational phases.

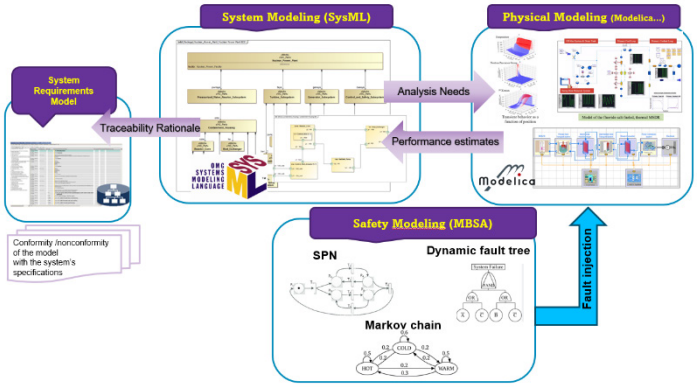

Figure 1: Framework architecture of the methodology proposed.

The methodology bridges two complementary domains: the MBSE environment, which manages the system architecture, requirements, and traceability, and the behavioral (physical) modeling environment, which simulates the system's dynamic response. The integration of these two domains allows the exchange of functional analysis with performance evaluation, ensuring that requirements, including safety-related ones, are continuously verified throughout the system's lifecycle.

USE CASE: MOLTEN SALT REACTOR

The proposed methodology is applied to a Molten Salt Reactor (MSR) concept, an advanced nuclear system in which liquid fuel circulates within a molten salt mixture (Xie et al., 2023).

A dynamic physical model of the MSR (Greenwood et al., 2018) was developed in Dymola using Modelica (Elmqvist et al., 1999) to represent the main reactor subsystems and their interactions. In this work, the primary pump is selected for degradation analysis because its performance directly affects critical safety variables such as coolant flow rate and core temperature.

MBSE ENVIRONMENT AND REQUIREMENTS

This study focuses on the Primary Fuel Loop, comprising the primary pump, reactor core, and primary heat exchanger, which collectively control molten salt circulation and heat transfer.

A simplified requirement model associated with the PFL is presented in Figure 2 using SysML (Friedenthal et al., 2006). These requirements reflect key functional and safety objectives and form the basis for subsequent verification under nominal and degraded operating conditions.

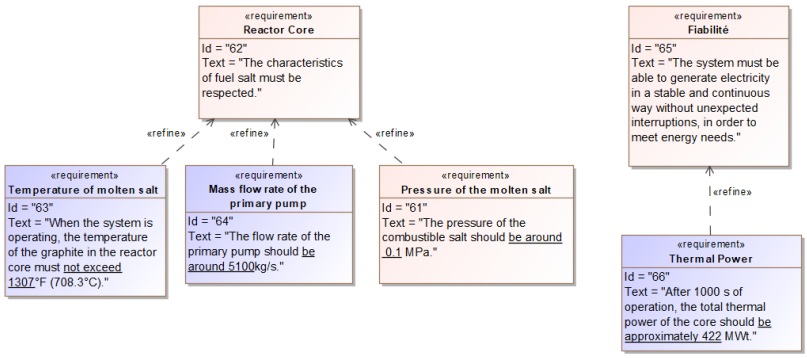

Figure 2: High level requirement diagram of PFL used for demonstrating the methodology.

PHYSICAL SIMULATION AND VERIFICATION MODEL

The detailed dynamic model of the MSR computes time-dependent variables such as temperature, pressure, mass flow rate, and reactor power, enabling evaluation of system behavior under nominal and degraded conditions (Figure 3). It accepts external inputs including control actions and fault triggers.

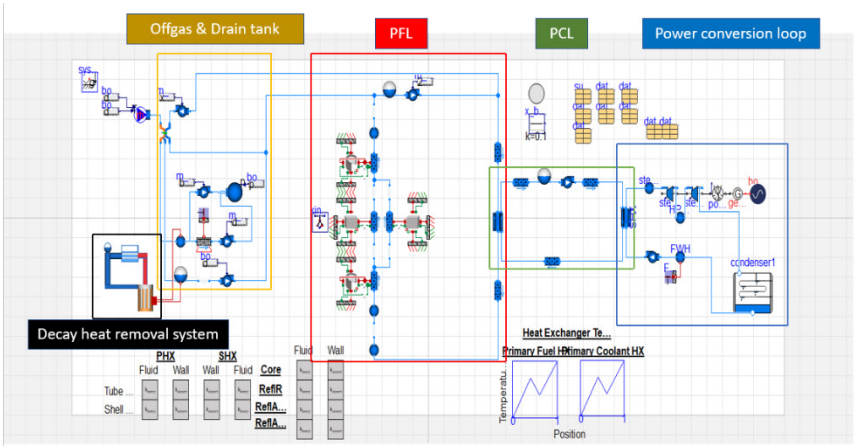

Figure 3: Physical model of MSR described in Dymola.

To enable automated verification, the verification model shown in Figure 4 integrates the CRML, a formalism developed to represent system requirements as executable models within the Modelica environment (Bouskela et al., 2023). Requirements are expressed as executable logical and temporal constraints directly linked to physical variables (e.g., core temperature, thermal power, pump flow rate). During simulation, CRML evaluates requirement satisfaction in real time using a four-valued logic system (True, False, Undefined, Undecided).

An observation model extracts relevant simulation signal, preprocesses them if necessary, and binds them to the corresponding requirement blocks. The resulting logical outputs are recorded and transferred to the MBSE environment to ensure traceable verification.

To assess degraded scenarios, a Stochastic Petri Net (SPN) module is integrated to model probabilistic wear-out of the primary pump. This enables unified verification of requirements under both nominal and stochastic degradation conditions.

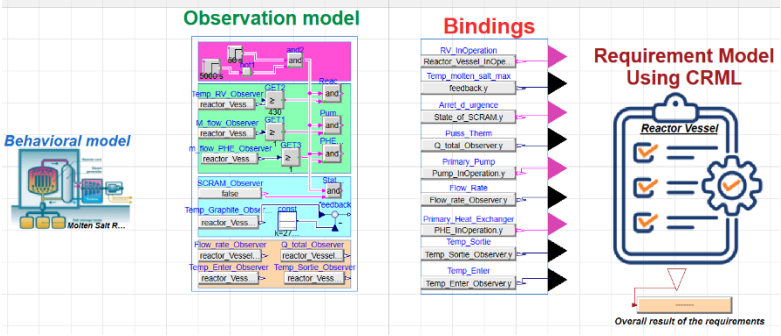

Figure 4: Verification model.

CO-SIMULATION INTEGRATION

The co-simulation architecture (Figure 5) synchronizes the physical model with the Catia Magic MBSE environment. During execution, Dymola computes system dynamics and evaluates CRML requirements, while Catia Magic monitors performance variables and requirement compliance at the system level.

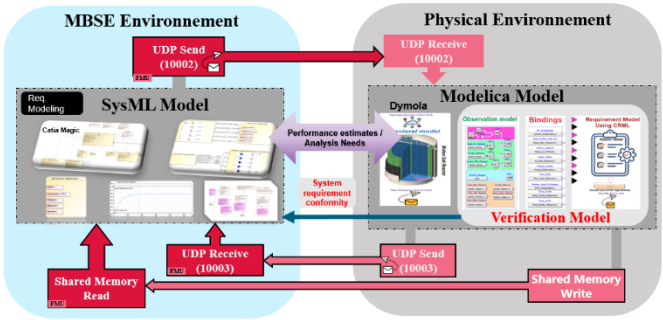

Figure 5: Data synchronization between Dymola and Catia Magic (MBSE).

Two categories of data are exchanged: (1) physical performance variables (e.g., pump flow rate, reactor power, core temperature), and (2) requirement verification results generated by the CRML requirement model. Real-time communication is achieved via UDP, while shared memory ensures reliable transfer of discrete verification results.

The Dymola communication models are exported as Functional Mock-up Units (FMUs) and integrated into the SysML architecture. Within Catia Magic, these FMU blocks receive simulation outputs and connect to parametric diagrams and constraint blocks. Python scripts convert numerical inputs into Boolean4 states for requirement visualization and compliance tracking.

After simulation, results are automatically recorded in the MBSE environment. A requirement traceability table (Figures 6) links each system requirement to its verification outcome, providing a formal compliance record and ensuring consistency between dynamic simulation results and system architecture.

#	Name	Text	Satisfied By	referredElements
1	34 Functioning of Control Rods	Upon receipt of an emergency shutdown (scram) signal, the system shall insert all control rods from the fully withdrawn position to the fully inserted position within 10.0 seconds or less, under normal operating conditions (nominal reactor pressure and temperature).	Core	R3 : String =
2	17 Flow Rate of the Primary Pump	The flow rate of the primary pump should be around 5100 kg/s.	Primary Pump	R4 : String =
3	19 Temperature of the graphite	When the system is operating, the temperature of the graphite in the reactor core must not exceed 1307°F (708.3°C).	Core	R1 : String
4	16 Thermal Power	After 1000 s of operation, the total thermal power of the core should be approximately 422 MWt.	Core	R2 : String =
5	68 The primary cooling salt outlet	The temperature of the salt exiting the heat exchanger should be approximately 839K (565.85°C)	Core	R6 : String =
6	67 The primary cooling salt inlet	The temperature of the salt entering the heat exchanger should be approximately 813K. (539.85°C).	Core	R5 : String =

Figure 6: Requirement table.

SAFETY MODELING

The degradation of the primary pump is modeled using a Stochastic Petri Net (SPN), which allows representation of progressive wear-out and probabilistic failure events (Bause and Kritzinger, 2002). SPNs are well suited for dynamic reliability modeling because they can represent time-dependent degradation processes (Norris, 1998).

In this study, degradation transitions follow a Weibull distribution to capture the progressive aging behavior of the pump (Klutke, 2003). The stochastic transitions trigger changes in the operational state of the pump over time.

To link the reliability model with the physical simulation, interface blocks map the SPN states (functional, warning, wear-out, and failed) to different pump performance levels (Figure 7). These states modify the pump mass flow rate, allowing degradation events to directly influence the thermal-hydraulic behavior of the reactor during co-simulation.

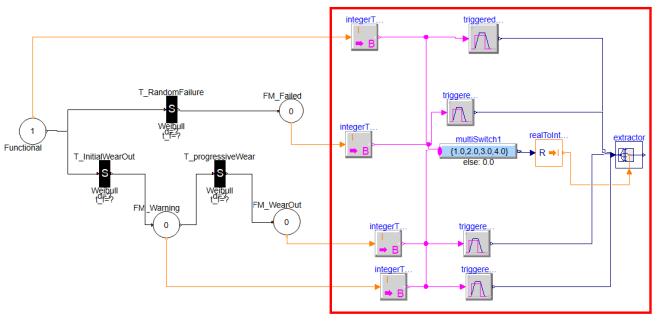

Figure 7: SPN with connecting blocks.

This configuration allows the physical model to respond dynamically to stochastic degradation events, linking failure behavior directly to system-level safety analysis during co-simulation.

RESULTS AND DISCUSSION

Co-Simulation Overview

The co-simulation was executed for over 5000 s to capture both nominal and degraded reactor behavior. Dymola computed the thermal-hydraulic response of the Primary Fuel Loop and the SPN degradation model, while Catia Magic performed system-level monitoring and requirement tracking. Real-time data exchange was achieved via UDP (Cloudflare Learning Center, 2025) for performance variables and shared memory for requirement states, confirming stable synchronization between environments.

Functional Scenario

Three key requirements were selected to assess nominal performance:

- R1: Core graphite temperature ≤ 708 °C (981.15 K)
- R2: Core thermal power ≈ 422 MWt after 1000 s
- R4: Primary pump flow rate ≈ 5500 kg/s

Under nominal conditions (Figure 8a), the pump flow stabilized near 5500 kg/s, core temperature reached steady-state around 660 °C (below the safety limit), and thermal power converged to approximately 422 MWt.

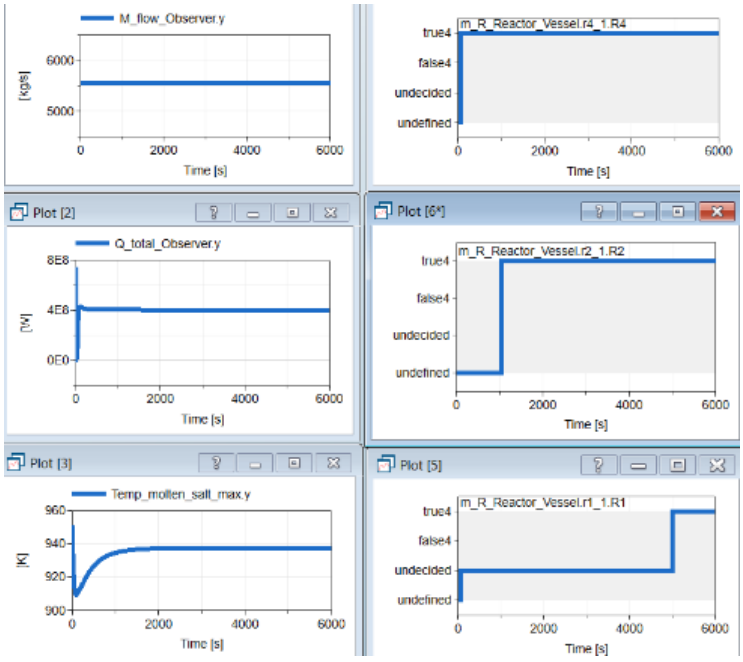

Figure 8: Simulation results showing physical behaviour (a) and requirement evaluation (b) under functional scenario.

CRML evaluation (Figure 8b) showed the expected transition sequence (Undefined → Undecided → True4) during system initialization and stabilization. Once steady-state conditions were reached, all three requirements were dynamically verified as **True4**, confirming compliance.

The same results were transmitted to Catia Magic via FMU integration. The MBSE verification table (Figure 9) confirmed full requirement satisfaction, demonstrating consistent traceability between physical simulation outputs and system-level requirement models.

Satisfied By	Bounds	referredElements
Core	=839	R6 : String = False4
Core	=813	R5 : String = True4
Primary Pump	=5100	R4 : String = True4 ←
Core	<=10	R3 : String = Valeur inconnue
Core	=422	R2 : String = True4 ←
Core	<=1307	R1 : String = True4 ←

Figure 9: Verification table.

Degraded Scenario

To assess degraded operation, the SPN model was activated during the 5000 s co-simulation to introduce stochastic pump degradation. Transition firing times occurred at approximately 10.9 s, 11.1 s, and 27.4 s, after which the pump entered a wear-out state and its performance declined.

As shown in Figure 10, the pump flow rate decreased from ~5500 kg/s to 3326.34 kg/s. Consequently, core temperature increased to approximately 734 °C (exceeding the 708 °C limit), and total thermal power rose to nearly 499 MWt.

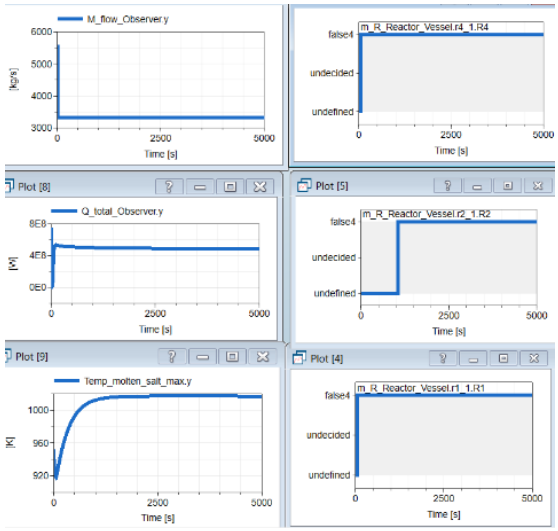

Figure 10: Simulation results showing the physical behavior (a) and requirement evaluation (b) under degraded conditions.

These results demonstrate that pump degradation significantly disturbed the reactor's thermal–hydraulic equilibrium.

CRML evaluations (Figure 10b) reflected this deviation in real time. At the start of the simulation, all requirements are in the Undefined state, as the system is still initializing, and the monitoring conditions have not yet been activated.

As the primary loop stabilizes, the requirements progress to Undecided, indicating that the evaluation criteria are being actively monitored but not yet fully validated. After the stochastic degradation events triggered by the SPN, the system starts deviating from its nominal operating point, and this change is immediately reflected in the CRML evaluations.

The logical transitions were directly aligned with physical parameter changes, confirming correct propagation of SPN-driven faults into the verification framework.

The same behavior was observed in the MBSE environment (Figures 11), where FMU-transmitted data updated the SysML verification table automatically. All affected requirements transitioned from True4 to False4, ensuring full traceability between stochastic degradation, physical response, and system-level compliance status.

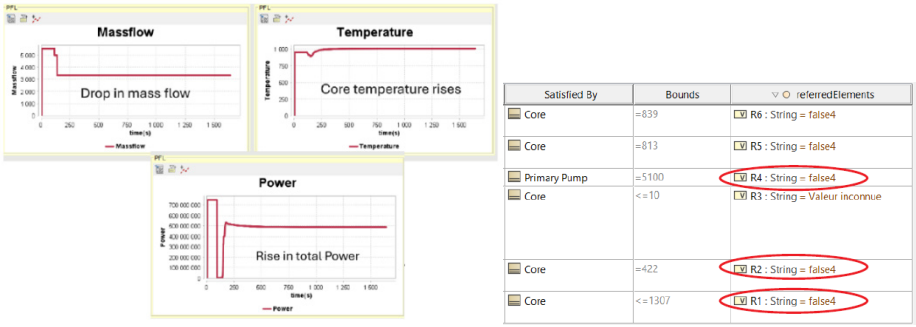

Figure 11: Catia magic simulation results under degraded scenario.

CONCLUSION

This study presented an integrated framework combining MBSE, Multiphysics simulation, CRML-based requirement verification, and Stochastic Petri Net degradation modeling for dynamic safety assessment of a Molten Salt Reactor. By coupling Dymola and Catia Magic through real-time co-simulation, the approach enables continuous and traceable verification of safety requirements under both nominal and degraded conditions.

Applied to a Molten Salt Reactor case study, the framework demonstrated its capability to capture the impact of stochastic degradation of the primary pump on system behavior. The results showed significant safety margin erosion, including reduced mass flow, increased core temperature beyond safety limits, and deviations in thermal power. These changes were automatically detected and consistently traced within the MBSE environment, supporting early identification of performance and safety deviations.

The methodology is generic and adaptable to other safety-critical domains. Future work will focus on scalability to multi-component systems, enhanced co-simulation performance, and the integration of product line engineering and system replication strategies.

REFERENCES

Bause, F. and Kritzinger, P.S. (2002). Stochastic Petri nets, Vol. 1. Wiesbaden: Vieweg.

Bouskela, D., Buffoni, L., Jardin, A., Molnar, V., Pop, A. and Zavada, A. (2023). The common requirement modeling language. Proceedings of the 15th International Modelica Conference, Aachen, Germany, pp. 497–510. https://doi.org/10.3384/ecp204497

Bouskela, D., Falcone, A., Garro, A., Jardin, A., Otter, M., Thuy, N. and Tundis, A. (2022). Formal requirements modeling for cyber-physical systems engineering: An integrated solution based on FORM-L and Modelica. Requirements Engineering, Vol. 27, pp. 1–30. https://doi.org/10.1007/s00766-021-00359-z

Cloudflare Learning Center (2025). User datagram protocol (UDP). https://www.cloudflare.com/fr-fr/learning/ddos/glossary/user-datagram-protocol-udp/ (accessed 28 May 2025).

Elmqvist, H., Bachmann, B., Boudard, F. and Vangheluwe, H. (1999). Modelica: A unified object-oriented language for physical systems modeling — tutorial and rationale. Report.

Friedenthal, S., Moore, A. and Steiner, R. (2006). OMG systems modeling language (OMG SysML) tutorial. INCOSE International Symposium, Vol. 9, pp. 65–67.

Greenwood, M.S., Betzler, B.R. and Qualls, A.L. (2018). Dynamic system models for informing licensing and safeguards investigations of molten salt reactors. Report ORNL/TM-2018/876. Oak Ridge, TN: Oak Ridge National Laboratory. https://doi.org/10.2172/1456790

Gyasi, S. and Akmali, M. (2025). Reliability and degradation analysis of complex systems using stochastic Petri nets and Monte Carlo simulations in Modelica.

Kaslow, D., Soremekun, G., Kim, H. and Spangelo, S. (2014). Integrated model-based systems engineering (MBSE) applied to the simulation of a CubeSat mission. Proceedings of the 2014 IEEE Aerospace Conference, Big Sky, MT, USA, pp. 1–14. https://doi.org/10.1109/AERO.2014.6836317

Kleyner, A. and Volovoi, V. (2010). Application of Petri nets to reliability prediction of occupant safety systems with partial detection and repair. Reliability Engineering & System Safety, Vol. 95, No. 6, pp. 606–613. https://doi.org/10.1016/j.ress.2010.01.008

Klutke, G.A., Kiessler, P.C. and Wortman, M.A. (2003). A critical look at the bathtub curve. IEEE Transactions on Reliability, Vol. 52, No. 1, pp. 125–129. https://doi.org/10.1109/TR.2002.804492

Modelica Association (2014). Functional mock-up interface for model exchange and co-simulation, Version 2.0.

Montgomery, D.C. and Runger, G.C. (2018). Applied statistics and probability for engineers, 7th ed. Hoboken, NJ: Wiley, pp. 482–485.

Norris, J.R. (1998). Markov chains. Cambridge, U.K.: Cambridge University Press.

Topper, A. and Horner, D. (2013). Model-based systems engineering in support of complex systems development. Johns Hopkins APL Technical Digest, Vol. 32, No. 1, pp. 419–432.

Xie, C., Luo, R., Revankar, S.T. and Yu, T. (2023). Controller design and stability analysis of an MSR plant based on a nonlinear distributed-parameter model. Applied Sciences, Vol. 13, No. 9, 5480. https://doi.org/10.3390/app13095480