Received 7 November 2025
Revised 8 December 2025
Accepted 10 December 2025

A systematic review of MBSE-based safety analysis techniques in railway systems

Jiaxu Chen
Railway Science and Technology Research and Development Center, China Academy of Railway Sciences Corporation Limited, Beijing, China

Abstract

Purpose – With the development of railway systems towards intelligence, informatization and networking, their architecture design becomes increasingly complex. Traditional safety analysis methods (such as failure mode and effects analysis (FMEA), fault tree analysis (FTA) and event tree analysis) can no longer realise integrated safety analysis across disciplines, domains and life cycles amid requirement drift, architecture iteration and operational scenario evolution. This paper aims to introduce a systematic, integrated, model-driven safety analysis framework for the entire life cycle of railway systems to address these complex safety challenges and improve the overall safety level of railway systems.

Design/methodology/approach – First, the paper conducts a literature review of traditional railway safety analysis techniques and their applications, and analyzes the technical framework, core elements (modelling languages, methods, and tools), and advantages of Model-Based Systems Engineering (MBSE). Then, it studies the integration of MBSE and system safety analysis, focusing on typical international research cases (e.g., the Methodology for the Description and Safety Analysis of Interoperable Systems (MeDISIS), the European Train Control System (ETCS) safety verification project SafeSysE, and the Reference Architecture for Model-Based System and Software Engineering in the Railway Domain (RAMSAS), etc.) and domestic research progress, and summarizes the core idea of integrating MBSE with safety analysis in the design process. Finally, it explores the key technologies of MBSE-based railway system safety analysis, including automatic mapping of architecture models to Fault Tree Analysis (FTA), dynamic linkage between behaviour models and Failure Mode and Effects Analysis (FMEA), multi-model collaboration and dynamic update, as well as technologies in three aspects: safety requirement analysis driven by railway operational tasks, integrated safety-function design analysis, and simulation-based safety verification via train-fleet operation modelling. The development and validation platform Platform for Integrated Systems and Mechatronic Engineering (PRISME) and tools such as the Dependability Engineering and Innovation System (DEIS), Behavior-Driven Development (BDD) frameworks, and International Business Machines (IBM) engineering suites were also utilized to support this research.

Findings – The MBSE-based railway system safety analysis technique embeds safety activities into the forward-engineering workflow of MBSE-driven development, enabling concurrent safety and functional design. It solves the problems of model heterogeneity, data silos and process discontinuities in traditional safety analysis and realises end-to-end traceability and consistency from system requirements to safety analysis results. This technique not only provides a rigorous foundation for standardised, efficient and accurate safety assessment of railway systems but also offers technical support for early identification of potential safety issues, reduction of late-stage design changes and continuous optimisation of system safety performance.

Originality/value – The innovation of this paper mainly includes three aspects:(1) It breaks the limitations of traditional document-driven safety analysis methods, constructs an MBSE-based integrated safety analysis framework covering the entire life cycle of railway systems and turns safety work from an ad-hoc add-on into a systematic, goal-oriented activity. (2) It proposes key integration technologies such as automatic mapping of SysML-based architecture models to FTA, dynamic linkage between behaviour models (state machine diagram/activity diagram) and FMEA and multi-model (FTA/FMEA/hazard and operability analysis)

Railway Sciences
Vol. 5 No. 2, 2026
pp. 276-287
Emerald Publishing Limited
e-ISSN: 2755-0915
p-ISSN: 2755-0907
DOI 10.1108/RS-11-2025-0051

Funding: This work was supported by the Science and Technology Research and Development Program of China National Railway Corporation Limited (Grant No. N2024T008). We are grateful for their financial support, which enabled this research.

Declaration of conflicting interests: The author(s) declare no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

collaborative dynamic update, which guarantee the consistency and traceability of safety analysis data and improve the efficiency of safety analysis iteration. (3) It develops a set of MBSE-based railway safety analysis implementation paths, including task-driven safety requirement decomposition, integrated safety function failure propagation modelling and train-fleet operation simulation-based verification, providing a practical technical solution for the safety design and analysis of complex railway systems.

Keywords Railway, Model-based systems engineering (MBSE), Safety analysis technology, Model-driven, System integration

Paper type Literature review

1. Introduction

Railway system safety is a key indicator of operational quality and service reliability and a strategic prerequisite for the continuous, stable and healthy operation of the country's transportation infrastructure. As the railway system progresses towards intelligence, informatization and networking, its requirements are constantly changing and architecture design becomes increasingly complex (Qin *et al*., 2019). Traditional safety design methods based on failure mode and effects analysis (FMEA), fault tree analysis (FTA) or event tree analysis (ETA) are unable to achieve integrated safety analysis across disciplines, domains and life cycles during requirement drift, architecture iteration and operational scenario evolution. Therefore, it is urgent to introduce a systematic, integrated and model-driven safety analysis framework for the entire railway system life cycle to address these increasingly complex safety challenges.

1.1 Literature review

Commonly used railway safety analysis techniques include failure modes, effects and criticality analysis (FMECA), FTA, ETA, Petri nets and Bayesian networks. FMECA enumerates component failure modes, evaluates their system-level effects and assigns severity levels. FTA links basic events to the undesired top event through a graphical logic diagram (Zhang, Wang, & Feng, 2023). ETA starts from an initiating event and branches to quantify the probabilities of subsequent outcomes (Fan, Yu, Liao, Sun, & Xi, 2018). Petri nets describe concurrent and synchronous behaviour, permitting simulation of train operation and signalling processes under various scenarios (Wang, 2022). Bayesian networks represent conditional dependencies among random variables, supporting risk assessment and decision-making under uncertainty (Kang, Zheng, & Niu, 2018). Combined application of these methods characterises the safety properties of railway systems and improves overall performance; their validity and utility are well established in both research and practice.

Valis and Koucky (2011) applied an enhanced FMECA to perform a risk assessment of the ETCS Level-2 system and identified its critical effects and latent hazards (David *et al*., 2010). Chang *et al*. introduced an integrated weighting algorithm to improve railway signal safety risk analysis (Liu, Yang, Cui, & Yang, 2020). Liu *et al*. (2020) constructed an FTA with railway system failure as the top event and calculated the corresponding failure probability (Liu *et al*., 2025). Chen, Yan, and Liu (2024) defined rules for converting fault tree models to binary-decision-diagram models and proposed an improved multi-state multi-valued decision-diagram method to analyse the failure probability of high-speed-railway traction-power-supply systems (Chen *et al*., 2024).

1.2 Motivation and contributions

Model-based systems engineering (MBSE) is a systematic modelling approach that constructs models to improve system design quality, reduce cost and risk and shorten development cycle time. In contrast to traditional systems engineering, MBSE establishes multi-level, multi-view models that provide comprehensive support for requirements analysis and management, overcome the limitations of current modelling techniques in requirements analysis and architecture design and are widely applied in defence and aerospace industries (Hu, Wang, Wang, & Fu, 2020).

MBSE-based railway safety analysis embeds safety activities within the forward-engineering workflow of MBSE-driven development, enabling concurrent safety and functional design. By examining MBSE fundamentals and its railway applications, we propose an integrated modelling and safety analysis technique for railways; the associated key technologies supply a systematic methodological framework, raising overall railway safety.

2. Analysis of the current state of MBSE technology research

2.1 Model-based system engineering technology

The MBSE technical framework underpins requirements, design, analysis, verification and validation (V&V) activities, thereby spanning the entire life cycle from concept design through development and into subsequent operational phases (Zhu, Yang, Gao, & Yao, 2016). The corresponding process flow is illustrated in Figure 1. MBSE is the ensemble of related processes, methods and tools employed for systems engineering in a model-based environment (Delligatti, 2013); its deployment hinges on three principal elements: modelling languages, modelling methods and modelling tools (Friedenthal, Moore, & Steiner, 2014).

In the system design phase, MBSE employs models to execute the technical activities of systems engineering, thereby minimising requirement-transfer errors and enabling multi-disciplinary collaborative design. MBSE models describe and analyse system states, behaviours and interactions under defined scenarios and tasks; these models are used to verify and derive functional requirements and logical architectures, accommodate requirement changes rapidly and guide subsequent detailed design, production, testing and verification activities (Figure 2).

Presently, MBSE models of system requirements, architecture and behaviour are built with SysML; the corresponding model structure is summarised in Figure 3 (Wolny, Mazak, Carpella, Geist, & Wimmer, 2020). Behavioural views comprise activity diagrams (behaviour flow), sequence diagrams (inter-module interactions during behaviour execution), state machine diagrams (system state transitions) and use-case diagrams (required system functions) (Friedenthal *et al.*, 2014).

In complex system development, MBSE offers three concrete advantages. First, it decomposes and traces requirements through multi-view, multi-level models, creating an unbroken path from top-level mission requirements to intermediate product requirements and, ultimately, to low-level component physical specifications. Second, its standardised modelling syntax yields a single, consistent data set that all disciplines can share during collaborative

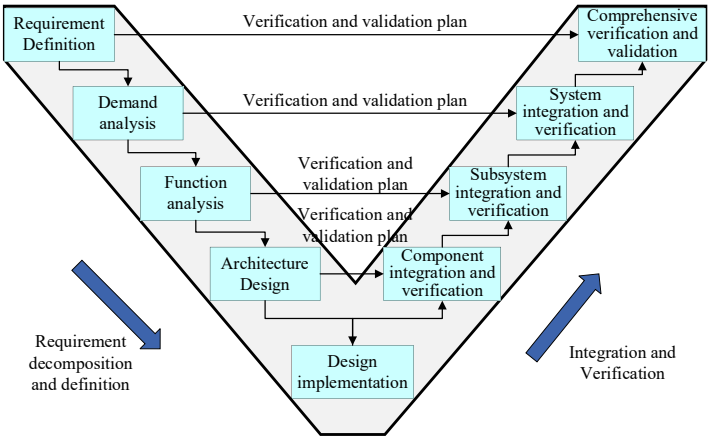

Figure 1. Model-based system engineering flow diagram. Source: Author's own work

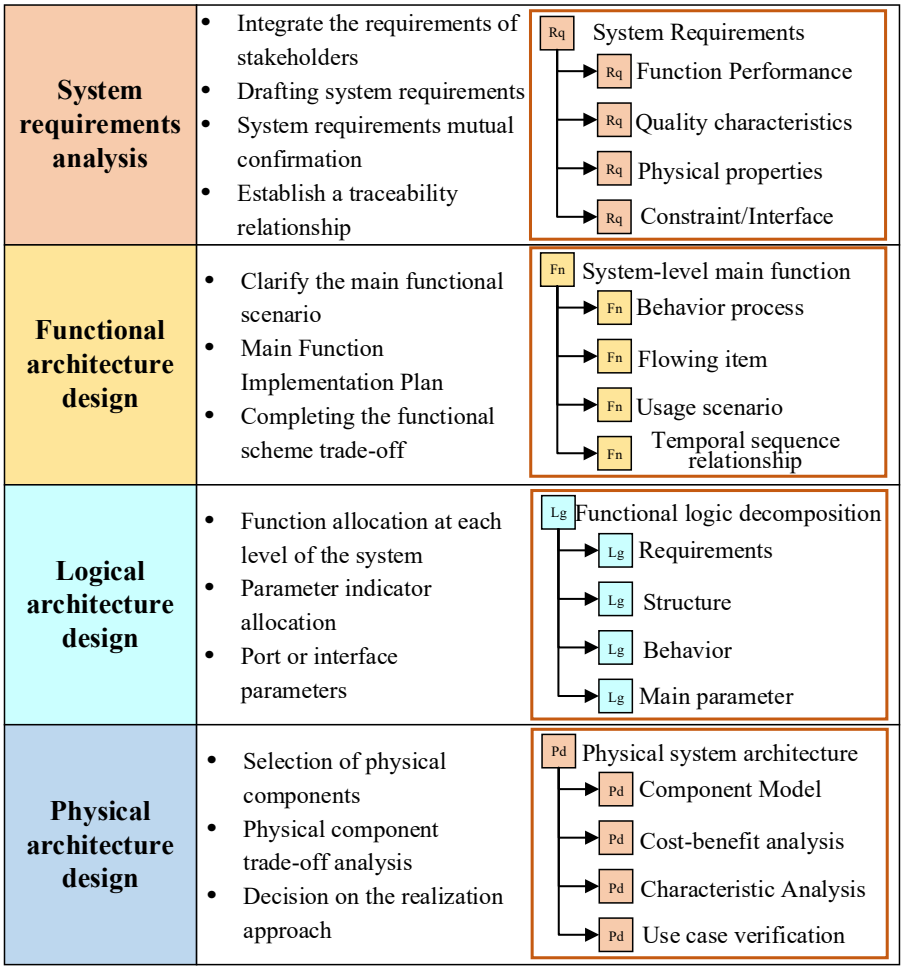

Figure 2. The hierarchical process and element decomposition diagram for MBSE system architecture design. Source: Author's own work

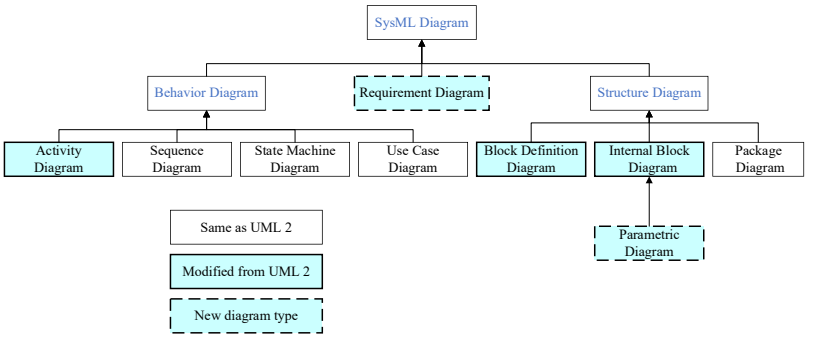

Figure 3. SysML model composition diagram. Source: Wolny *et al.* (2020)

design. Third, MBSE integrates diverse simulation techniques, enabling multi-domain, multi-physics and high-fidelity analyses early in development.

The approach is already operational in aerospace, defence and automotive programmes. The "systems engineering ellipse" model, for instance, iterates through requirement definition, system analysis, design, implementation and verification, with explicit feedback loops between life cycle stages. Likewise, automotive functional-safety standard International Organization for Standardization 26262 mandates that safety analyses proceed in parallel with development and that a complete safety case be delivered for review (Cuenot, Ainhauser, & Adler, 2014) (Figure 4).

3. Research on the integration of MBSE and system safety analysis

In the early phases of systems engineering development, both researchers and industry focused on merging safety, structural and behavioural models into a single framework that would allow safety and performance to be analysed together, with the goal of improving analytical accuracy and efficiency. At that time, however, modelling technology was immature: no universally accepted modelling language existed, and modelling methods lacked standardisation. Consequently, the field splintered into several strands that relied on incompatible functional models, most of which lay outside mainstream design practice, thereby limiting the wider adoption of model-based safety analysis.

MBSE provides the technical scaffolding needed to embed safety and reliability analyses into every phase of system development. By prescribing clear objectives and well-defined inputs/outputs for each stage, MBSE turns safety work from an ad-hoc add-on into a systematic, goal-oriented activity. Equally important, MBSE delivers a single, authoritative digital model that serves as the sole data source for all downstream analyses. This eliminates the heterogeneous and often inconsistent functional models that historically plagued safety studies, guaranteeing that safety analysts and performance designers operate on identical, fully synchronised data. The resulting homogeneity at the data level is a prerequisite for rigorous, repeatable and traceable model-based safety analysis.

In this research direction the dominant approach is to follow the MBSE design flow and use model integration and/or mapping to achieve joint development of system function and safety.

The French PRISME laboratory proposed MeDISIS (David, Idasiak, & Kratz, 2010), a reliability and safety analysis process aligned with mainstream MBSE. In the requirements

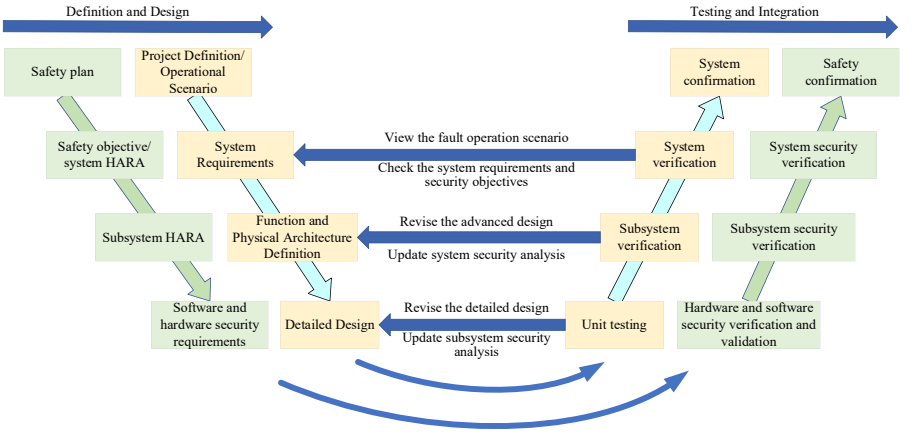

Figure 4. Automotive industry standard V model development process. Source: Cuenot *et al.* (2014)

stage, preliminary hazard analysis defines functional failure states; during functional analysis, functional FMEA derives additional design requirements; in the design-integration stage, component FMEA, performance-reliability analysis and fault-injection verification are performed to evaluate and refine the architecture.

Mhenni presented SafeSysE, an MBSE-integrated safety method (Mhenni, Choley, Nguyen, & Frazza, 2016). In requirements analysis a top-level function list is established and subjected to functional-risk analysis; in functional design functional FMEA is executed to identify critical functional failures and to formulate safety-derived requirements; in architecture design preliminary component FMEA is carried out to verify whether the architecture controls functional faults and to optimise the design (Figure 5).

The DEIS group at the University of Calabria proposed RAMSAS (Alfredo & Andrea, 2012), a four-step reliability, availability, maintainability and safety analysis and simulation method (requirements analysis → system modelling → system simulation → system evaluation) that is iterated throughout the design process; the method is simulation-centred and does not include early-architecture reliability analysis.

Xie developed an MBSE-centric reliability and safety design and analysis process that links the equipment design model and the reliability/safety model bidirectionally, enabling concurrent design and reliability and/or safety work (Xie *et al*., 2025). Wang, Qin, and Liu (2024) addressed the all-electronic safety system of torpedoes. Building on conventional safety and reliability analysis, they developed a safety system modelling procedure grounded in systems engineering. Functional requirements, system architecture, activity views and temporal-logic control were adopted as the constituent elements for safety and operational-reliability analysis, and fault propagation was modelled within the system functional model (Wang *et al*., 2024). Qi, Jin, Peng, Zhang, and Cai (2024), adopting a model-based systems engineering perspective, proposed a method that identifies potential faults concurrently along three dimensions – function, performance and structure – during the forward-design and modelling phases of complex systems (Qi *et al*., 2024).

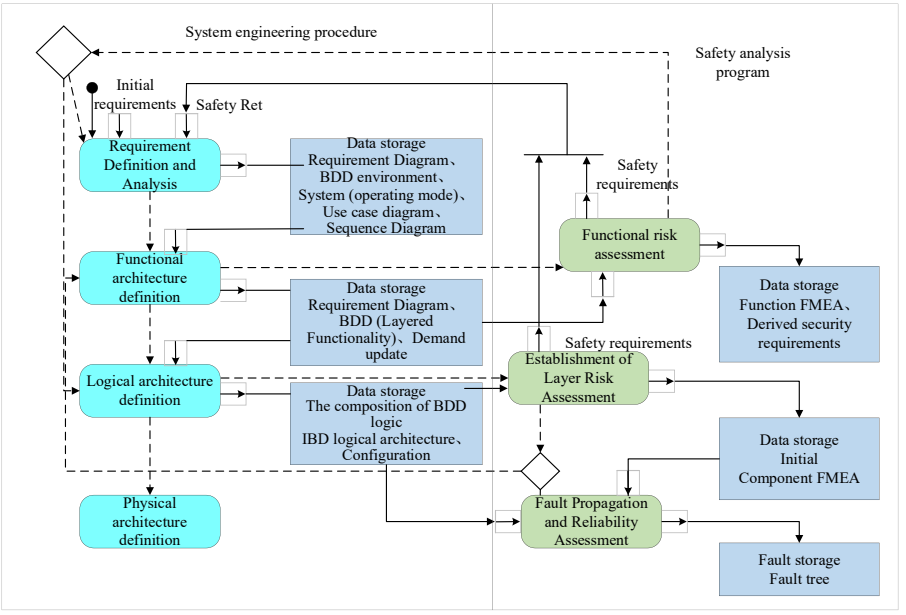

Figure 5. Integration process of SafeSysE. Source: Mhenni *et al.* (2016)

Overall, the main idea of integrating MBSE and system safety analysis in the design process is as follows: during the system requirements analysis phase, the system function list and usage requirements in the MBSE model are used to conduct preliminary functional failure analysis and hazard analysis, refining safety requirements; in the system function analysis and logical architecture design phase, a comprehensive analysis model is built on the basis of the system normal function model with the support of the fault mode database, focusing on architecture improvement; after the system physical architecture design is completed, dynamic simulation evaluation of the system normal and fault behaviours is carried out, further optimising the fault control logic and algorithms of the system.

4. Research on safety analysis technology of railway systems based on MBSE

4.1 Integrated key technologies for safety analysis method of railway system based on MBSE

MBSE leverages standardised modelling languages such as systems modelling language (SysML) to create a coherent, lifecycle-wide system model. By unifying requirements elicitation, architectural design, integration verification and operational optimisation within a single normative framework, MBSE eliminates the model heterogeneity, data silos and process discontinuities that plague conventional railway safety analyses. Consequently, it offers a rigorous foundation for standardised, efficient and demonstrably accurate safety assessment of railway systems.

(1) Automatic mapping of the architecture model to FTA

The fidelity of any fault tree analysis (FTA) is governed by the rigour with which system constituents and their interactions are encoded. In MBSE practice the block-definition diagram (BDD – a SysML artefact – serves as the canonical repository of this information. A single BDD captures the complete decomposition of the railway asset from top-level function to lowest replaceable unit, prescribes the interfaces between siblings and explicitly traces data and energy flows. The train braking system illustrates the principle: the BDD simultaneously declares the brake controller (brake-demand computation), the hydraulic actuator (pressure modulation) and the speed sensor (velocity feedback), while binding each element to its functional boundary, failure-relevant attributes and peer connectors. Such a structured, semantically rich description guarantees that the subsequent FTA is both complete and traceable to the system architecture.

By exploiting the automation capabilities of MBSE environments such as IBM Rhapsody, the system architecture model can be translated into a fault tree without human intervention. Model-transformation rules that map SysML to analysable languages (e.g. AltaRica 3.0) automatically generate the fault tree, eliminating the transcription errors inherent in manual construction. Because the same SysML source is reused, the functional definitions and component interactions captured during architecture design remain traceably consistent with the failure logic and event couplings elaborated in the subsequent safety analysis. This end-to-end consistency provides the rigorous, repeatable foundation required for standardised and efficient safety assessment of railway signalling systems.

(2) Dynamic linkage between the behaviour model and FMEA

Fault mode and effects analysis (FMEA) is a widely adopted method for safety verification in railway systems. Its primary objective is to systematically identify potential functional failure modes throughout the system's life cycle, analyse the root causes of these failures and quantitatively assess their impacts on system functionality, the operating environment and personnel safety. The accuracy of this analysis largely depends on a clear representation of the system's dynamic behavioural logic. Within MBSE, the state machine diagram and activity diagram of the SysML offer standardised modelling frameworks. Specifically, the SysML state machine diagram can accurately describe the behavioural patterns and state transition

conditions of a system or subsystem under various operating scenarios through discrete states and transitions. Meanwhile, the activity diagram visually illustrates the execution steps, resource dependencies and parallel or branching logic of system functions using process nodes and control flows. Together, these diagrams provide a comprehensive technical framework for modelling the dynamic behaviour of railway systems.

Focusing on the train dispatching system as a critical subsystem, its SysML State Machine model defines typical operational states – such as "normal dispatching," "temporary speed restriction," "fault downgrade" and "emergency takeover" – centred on the core dispatching functions and explicitly specifies the triggering conditions for transitions between these states. By extending the SysML profile, the behavioural model can be associated with failure modes, enabling the automatic generation of FMEA tables that include fields such as failure mode, cause and impact level (S/O/D). Through bidirectional "requirement–model" traceability, consistency between FMEA results and system implementation can be ensured. This traceability mechanism not only guarantees that the FMEA analysis covers all key functions and requirements but also establishes a dynamic link between FMEA outcomes and system design. When the behavioural model is modified due to requirement changes, the FMEA table can be automatically updated via tools, effectively avoiding the issues of information lag and inconsistency associated with traditional manual FMEA maintenance, thereby supporting the dynamic and accurate analysis of failures in railway systems.

(3) Multi-model collaboration and dynamic update

Complex railway systems exhibit deep hierarchical structures, tight functional coupling and highly dynamic operating contexts. A single safety analysis technique is therefore no longer capable of covering every risk dimension. A coherent combination of FTA, FMEA and hazard and operability analysis (HAZOP) is required to obtain mutually complementary coverage. MBSE eliminates the "information islands" generated by these stand-alone techniques by establishing a single, living model repository under a dynamic update regime. The repository enables concurrent model interaction and guarantees consistency across the entire life cycle, thereby supplying an integrated, model-driven backbone for the safety analysis of complex railway systems.

The unified model library acts as the core data carrier for multi-model collaboration; its value lies in standardised storage and cross-project reuse of safety analysis resources. The library contains common basic data modules for railway systems – typical failure-mode libraries for key train components (wheelsets, braking systems and traction inverters) and generic safety design templates – and a rule library for safety analysis methods, including the mapping between fault tree basic events and FMEA failure modes and the correspondence between HAZOP deviation scenarios and system behaviour model states. This structured approach allows project teams to retrieve standardised resources directly, eliminating repeated construction of basic models, reducing modelling cost and ensuring consistent safety analysis standards across projects.

The dynamic update mechanism is essential for ensuring the synchronised evolution of multiple models and system design. Its primary function is to enable the MBSE tool to trace inter-model relationships and automatically identify the scope of safety analysis models affected by design changes. Specifically, based on a predefined change impact analysis algorithm, the tool traverses nodes in the system architecture and behavioural models that depend on the modified elements, thereby locating affected fault tree branches in FTA, failure mode items in FMEA and deviation scenarios in HAZOP. For instance, when redundant communication channels are added to a train system, the tool identifies this design change and automatically introduces a new basic event branch in the FTA, representing "simultaneous failure of redundant communication channels." It then updates the top event's failure probability based on the reliability parameters of the new channels. Simultaneously, in the FMEA, it incorporates "redundant channel switching delay" as a new failure mode, includes its

impact on train operation safety and recalculates the corresponding risk priority number. This entire update process eliminates the need for manual inspection of individual models. It significantly shortens the safety analysis iteration cycle following design changes and reduces the risk of overlooking affected models, thereby ensuring dynamic consistency between system design and safety analysis. This capability effectively addresses the safety analysis challenges posed by frequent design iterations throughout the lifecycle of complex railway systems.

In addition, a dual-layer structure comprising a "core traceability chain" and an "associated traceability chain" is established. The core chain addresses safety-critical requirements – such as train braking and signal control – and enforces rigid, lifecycle-long traceability. The associated chain accommodates non-safety-critical functional extensions; it adopts a "requirement–module–verification result" pattern that shortens the traceability path by omitting redundant intermediate nodes. For example, when a train dispatching system is augmented with a non-safety-related data-statistics function, only the direct links among the functional requirement, its implementation module, and the corresponding test case are recorded; traceability to low-level hardware components is not required.

Concurrently, an automatic mapping rule base for traceability relations is defined by extending the SysML meta-model. Whenever requirements evolve, a plug-in developed for the MBSE platform (e.g. IBM Rhapsody) automatically identifies the scope of change: for functional-expansion requirements, new traceability links are created; for performance-optimisation requirements, the traceability attributes of the affected model nodes are updated and invalid links are removed. Version control and differencing capabilities are integrated to capture the change history of every traceability relation and to enable one-click rollback, thereby significantly reducing manual-maintenance overhead.

4.2 Key technologies for safety analysis of railway systems based on MBSE

MBSE transforms the traditional document-driven approach into a model-driven one by employing models as the primary means of information exchange and system specification throughout the system lifecycle. It supports functional analysis during the early stages of railway system design, facilitating the identification of potential issues and bottlenecks. Early detection helps minimise late-stage design changes. Additionally, simulation enables the evaluation of various operational scenarios and failure conditions, contributing to the verification that the system meets its safety objectives. The MBSE-based railway system safety analysis method integrates key technologies across three main areas: requirements analysis, comprehensive modelling and simulation-based verification.

(1) Safety requirement analysis driven by railway operational tasks

In railway safety analysis, task-oriented safety requirement analysis is essential to guarantee that both design and operation satisfy the specific demands of each operational task. Its primary objective is to create an accurate functional profile that maps system functions to railway operational tasks. In conventional design, the coarse granularity of task descriptions usually prevents such a mapping from being established with sufficient precision. MBSE overcomes this limitation by employing operational-view and functional-view models that tightly couple usage requirements with system requirements. The task-scenario model and the top-level functional model generated by MBSE are combined to produce a task-to-function mapping table. Building on this table, a functional failure analysis model is constructed to decompose high-level safety requirements down to individual system functions.

(2) Integrated safety–function design analysis

The objective is to derive a comprehensive failure propagation model that captures how faults originating in any constituent subsystem or component propagate through the railway system and degrade overall performance. Because railway systems are highly interconnected, a local

fault can escalate to system-level failure; quantifying these propagation paths is, therefore, central to safety analysis.

Using MBSE, we embed component failure modes directly into the system functional model, quantify their effects on each output and link these local failure data into a unified model that couples function design with safety analysis. The resulting model automatically yields the fault-logic structure of the railway system and supports subsequent safety assessment.

Model construction proceeds in four steps.

(1) *Baseline functional model extraction.* Core MBSE artefacts – functional operations, functional timing and system composition – are extracted and organised into a hierarchical, nominal-function model.

(2) *Local failure-logic definition.* For each unit, the local input–output failure relation, internal state transition function, temporal and logical fault dependencies and any functional reconfiguration behaviour are formally specified.

(3) *System-level failure model integration and validation.* Local failure-logic blocks are composed into the global failure propagation model, which is then verified for completeness and consistency against the baseline functional model.

(4) *Automatic generation of fault-logic structures.* Causal relationships encoded in the integrated model are exported as fault trees, Bayesian networks or FMEA/FMECA tables, enabling exhaustive analysis of single and combined failure scenarios.

(3) Simulation-based safety verification via train-fleet operation modelling

Safety verification by simulation faces several practical challenges: accurate modelling of complex systems, management of large data volumes, assurance of environmental fidelity, model V&V, integration of multi-disciplinary knowledge, interpretation of results, selection or development of suitable tools, efficient allocation of computational resources and demonstration of result reliability.

To address these issues, we propose a train-fleet operation simulation method for railway system safety verification. An MBSE-compliant model of the railway system – incorporating track topology, stations, signalling, rolling stock and supporting infrastructure – is first constructed so that its behaviour and performance match those of the real system. A simulation platform is then selected or developed to reproduce fleet operation under representative, abnormal and emergency conditions.

Hazardous events and accident scenarios are injected into the runs to observe system response, quantify accident likelihood and evaluate consequence severity. Simulation outputs are compared with theoretical predictions and field data to identify weak points and to prioritise design or operational improvements. Iterative V&V ensures that the model remains valid while the safety level of the railway system is progressively enhanced.

5. Conclusion

Increasing complexity and tighter integration in railways raise both the difficulty of safety analysis and the required safety level. To meet these challenges, we propose an MBSE-based railway safety analysis technique that employs systems engineering practices: safety requirements are decomposed and allocated through models that originate in the system requirement set, and both analytical calculations and simulation-based verification are performed. This approach provides end-to-end technical support for the safety design and analysis of railway systems. Future work should therefore concentrate on railway system requirements and design models, deepen the investigation of safety design procedures and methods within the MBSE framework and advance intelligent modelling techniques for

railway safety, thereby ensuring safe and reliable operation and improving overall railway safety performance.

Reference

Alfredo, G., & Andrea, T. (2012). A model-based method for system reliability analysis. In *Simulation Series-Part of the 2012 Symposium on Theory of Modeling and Simulation-DEVS Integrative M&S Symposium.*

Chen, J. X., Yan, S. S., & Liu, X. Q. (2024). Research on reliability analysis of high-speed railway traction substation system under common cause failures. Proceedings of the Institution of Mechanical Engineers, Part O. *Journal of Risk and Reliability, 239*(5), 1164–1177. doi: 10.1177/1748006x241291129.

Cuenot, P., Ainhauser, C., & Adler, N. (2014). Applying model based techniques for early safety evaluation of an automotive architecture in compliance with the ISO 26262 standard. In *Embedded Real Time Software and Systems (ERTS2014)* (pp. 20–11).

David, P., Idasiak, V., & Kratz, F. (2010). Reliability study of complex physical systems using SysML. *Reliability Engineering & System Safety, 95*(4), 431–450. doi: 10.1016/j.ress.2009.11.015.

Delligatti, L. (2013). *SysML, distilled: A brief guide to the systems Modeling Language*. Boston, MA: Addison-Wesley.

Fan, Y. W., Yu, G., Liao, K., Sun, J. J., & Xi, Y. W. (2018). Application of fault tree analysis method in risk analysis of freezing damage in tunnels of cold regions based on fuzzy numbers. *Safety and Environmental Engineering, 25*(6), 146–151.

Friedenthal, S., Moore, A., & Steiner, R. (2014). *A practical guide to SysML: The systems modeling language*. Waltham, MA: Morgan Kaufmann.

Hu, X. Y., Wang, R. P., Wang, X., & Fu, Y. T. (2020). Recent development of safety and reliability analysis technology for model-based complex system. *Acta Aeronautica et Astronautica Sinica, 41*(6), 523436.

Kang, Y. J., Zheng, Y. S., & Niu, X. T. (2018). Human reliability analysis based on SLIM and Bayesian network model under the abnormal conditions in the case of arrival and departure of trains. *Railway Transport and Economy, 40*(1), 56–62.

Liu, C., Yang, S. W., Cui, Y., & Yang, Y. X. (2020). An improved risk assessment method based on a comprehensive weighting algorithm in railway signaling safety analysis. *Safety Science, 128*, 104768. doi: 10.1016/j.ssci.2020.104768.

Liu, P., Fang, X., Chen, J., Zhang, J., Zhang, K., & Wang, M. (2025). Reliability allocation of railway system based on fault tree. *Railway Sciences, 4*(4), 550–562. doi: 10.1108/rs-06-2025-0020.

Mhenni, F., Choley, J. Y., Nguyen, N., & Frazza, C. (2016). Flight control system modeling with SysML to support validation, qualification and certification. *IFAC-PapersOnLine, 49*(3), 453–458. doi: 10.1016/j.ifacol.2016.07.076.

Qi, Y. Q., Jin, P., Peng, Q. B., Zhang, H. L., & Cai, G. B. (2024). Model-based fault identification and modeling method for space propulsion system. *Systems Engineering and Electronics, 46*(12), 4062–4073.

Qin, Y., Sun, X., Ma, X. P., Wang, M. M., Jia, L. M., & Tang, T. (2019). Research on the architecture of intelligent railway 2.0 and its applications. *Journal of Beijing Jiaotong University, 43*(1), 138–145.

Valis, D., & Koucky, M. (2011). RAMS program in rail applications-brief introduction. *Problemy Eksploatacji*, 1, 185–193.

Wang, M. (2022). Study on safety risk of external environment along high-speed rail based on Petri net model. *China Safety Science Journal, 32*(S1), 57–62.

Wang, C. X., Qin, D. Z., & Liu, Y. (2024). Safety and mission reliability analysis of torpedo electronic safety and arming system based on MBSE. *Computer Measurement & Control, 32*(4), 314–321, 340.

Wolny, S., Mazak, A., Carpella, C., Geist, V., & Wimmer, M. (2020). Thirteen years of SysML: A systematic mapping study. *Software and Systems Modeling*, *19*(1), 111–169. doi: 10.1007/s10270-019-00735-y.

Xie, L. M., Huang, D. J., & Wu, Z. G. (2025). Application research on reliability and safety analysis of fuel system based on MBSE model. *Electronic Product Reliability and Environmental Testing*, *43*(4), 19–27.

Zhang, D. R., Wang, K. M., & Feng, X. Y. (2023). Causal analysis of high-speed railway accidents based on knowledge graph and fault tree. *Railway Computer Application*, *32*(7), 14–18.

Zhu, J., Yang, H., Gao, Y. H., & Yao, T. K. (2016). Summary of model based system engineering. *Aeroengine*, *42*(4), 12–16.

Corresponding author
Jiaxu Chen can be contacted at: chenjiaxu168@163.com

Jiaxu Chen is an Assistant Researcher of China Academy of Railway Sciences Corporation Limited. He is mainly engaged in research on railway system safety risk analysis and evaluation, railway RAMS (Reliability, Availability, Maintainability and Safety) integrated design, analysis and modeling, railway system integration and comprehensive support technologies, etc. He has won the First Prize of Science and Technology Award of China Academy of Railway Sciences Corporation Limited and the 8th National Railway Youth Science and Technology Innovation Award.