Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27900-cd

A Systematic Approach for Determining and Verifying Hazards to Support ETCS Moving Block Safety Assessment

Araaf Recta[1], Julie Beugin[1], Rim Saddem-Yagoubi[2], Mohamed Ghazel[1]
[1]*Univ. Gustave Eiffel, COSYS, ESTAS, Villeneuve d'Ascq, France. E-mail: firstname.lastname@univ-eiffel.fr*
[2]*Aix Marseille Univ, CNRS, LIS, Marseille, France. E-mail: rim.saddem@lis-lab.fr*

Moving Block (MB) railway signalling enhances railway capacity through dynamic train separation based on real-time localisation and braking distances. These complex functional behaviours of MB systems, such as communication processes, and timing constraints, make safety assessment particularly challenging. Formal verification techniques, in particular model checking, are increasingly adopted in industry to prove the correctness of such safety-critical systems. However, to cope with the state explosion problem, verification models are often simplified, reducing their accuracy and limiting their applicability to realistic operational conditions. To address this limitation, we propose an integrated verification approach combining System-Theoretic Process Analysis (STPA) and Statistical Model Checking (SMC). STPA is used to identify relevant causal factors and hazardous operational scenarios, including disturbances such as delays and sensor errors, which are then explicitly incorporated into the formal model. Safety properties are subsequently analysed under these realistic conditions using UPPAAL SMC.

Keywords: Safety Analysis, Moving Block, Railway Signalling, Statistical Model Checking, STPA, UPPAAL.

1. Introduction

Moving Block (MB) signalling systems, as investigated within the European Research programmes Shift2Rail and Europe's Rail, constitute a key evolution of railway traffic management and control. Integrated into the European Train Control System (ETCS), MB systems enable dynamic train separation based on real-time localisation and braking distances, allowing trains to run closer together while maintaining safe separation and increasing network capacity.

As MB systems are safety-critical, formal verification techniques are increasingly adopted to analyse safety properties. However, when simplifications (abstractions) are introduced during the modelling of such complex systems, this can reduce the relevance of verification results in practice, especially where train positions are measured continuously in real time. Limiting the model's behaviour can also inadvertently eliminate executions that are critical for safety analysis (Pakonen et al., 2021).

In this paper, we address the problem of how to systematically construct and analyse safety-related operational scenarios in MB systems under realistic operating conditions. In particular, we investigate whether hazardous situations can be reached when causal factors (CFs) are explicitly taken into account.

To this end, we formalize safety-related scenarios by analysing relevant CFs that could trigger such hazardous situations using System-Theoretic Process Analysis (STPA). STPA is used to identify safety-relevant disturbances and interactions, which guide the construction of operational scenarios to be analysed. The identified CFs are then explicitly incorporated into the formal model to assess whether they can lead to hazards.

Verification is performed over bounded time horizons corresponding to a single operational mission, from the start of train movement until all trains stop. This bounded-time analysis enables the evaluation of system behaviour and safety properties under specific temporal constraints, without requiring reasoning over infinite mission durations. To cope with the combinatorial complexity of the behaviour space, UPPAAL Statistical Model Checking (SMC) (David et al., 2015) is used to analyse safety properties based on a non-exhaustive, statistical exploration of execution paths.

Several work have explored the combination of STPA and model checking as a means to support the analysis of safety-critical systems. Abdulkhaleq and Wagner (2014) proposed, for instance, an integration of STPA with SPIN model checker, applied to an adaptive cruise control system. However, their approach primarily focuses on translating control safety constraints into verification properties, and does not address the analysis of hazardous scenarios and CFs identified in the final STPA step. Tsuji et al. (2020) and Zhang and Liu (2018) combined STPA with UPPAAL, with application to a very specific Fixed Block case. In these works, scenarios and CFs are used to derive the properties to be verified, while the analysis remains centred on the correctness of control-command logic.

In contrast, the present work targets an ETCS Moving Block system and extends our previous study (Recta et al., 2025), in which the correctness of the control-command logic was already established. The considered system is characterized by dynamic train separation and continuous onboard–trackside interactions. Beyond control-logic correctness, the proposed approach enables the systematic analysis of hazardous situation reachability under realistic operational disturbance scenarios, such as delays and measurement errors.

The remainder of this paper is organized as follows. Section 2 introduces the ETCS MB signalling system, recalls the formal model developed in our previous work, as the basis for the present work, and outlines the safety assumptions. Section 3, presents the proposed STPA verification-approach and its integration with statistical model checking using UPPAAL SMC. Section 4 extends our previous work by analysing hazardous situation reachability in scenarios derived from STPA. Finally, Section 5, concludes the papers and presents perspectives.

2. ETCS MB Signalling: Modelling, and Safety-Related Assumptions

MB operation in the full MB variant of ETCS (previously referred to as Level 3, now considered within the scope of advanced Level 2 configurations) envisages the utilisation of GNSS technologies (Global Navigation Satellite System) for autonomous train localisation, relying on the availability of accurate and continuous train positions without trackside detection devices. This satellite-based localisation technology represents one of the most promising solutions, enabling real time and periodic transmission of a safe zone, referred to as Movement Authority (MA), computed by exploiting the estimated front-end and rear-end positions.

Preliminary safety analyses for ETCS MB systems were conducted within the Shift2Rail X2Rail projects (X2Rail-5, 2022). These analyses resulted in the identification and classification of hazards, together with potential mitigations and links to system requirements, forming a basis for the hazard log used in the railway safety assessment process. In the subsequent R2DATO project (Rail to Digital Automated , 2025), STPA was explored as a complementary approach to traditional railway hazard identification techniques (e.g., Preliminary Hazard Analysis) to capture hazards arising from interactions between system components and operational conditions.

However, hazard logs used in railway safety processes typically rely on expert judgement and scenario-based reasoning. As a result, they do not provide a formally grounded exploration of safety-critical system behaviours, nor do they directly lead to precise, verifiable safety properties.

To support the formal analysis of MB systems, our previous work developed a formal model of the ETCS MB system using UPPAAL (Recta et al., 2025). The model integrates train dynamics, communication mechanisms, route and point management, as well as train integrity supervision. Train integrity refers to the capability of confirming that a train is complete and non-fragmented, which is essential to correctly determine the rear-end position used in MA computation.

The model considers a scenario involving three trains operating on different routes, as illustrated in Figure 1, and is analysed under the Normal Train Movement Use Case (NTM-UC). This use case corresponds to nominal MB operating con-

ditions, in which train integrity is periodically confirmed and the driver follows the prescribed speed profile.

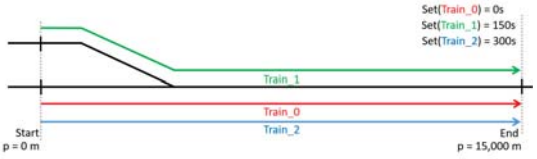

Fig. 1. Three Following Trains Case

These conditions rely on several safety-related assumptions, including the availability of accurate train localisation, periodic confirmation of train integrity, and reliable communication between onboard and trackside components. Within this nominal operating context, the model was shown to satisfy key safety properties: the absence of track overlapping and incorrect point (switch) positions.

In the present work, we extend this model by explicitly introducing the causal factors identified through STPA. This extension allows us to assess whether safety-relevant disturbances and timing effects identified through STPA are effectively handled by the system, or whether they can lead to hazardous situations, even in the absence of explicit component failure.

The following section details the methodology, starting with the application of the STPA steps.

3. STPA-Based Methodology

3.1. *System-Theoretic Process Analysis (STPA)*

STPA is a modern safety analysis technique aimed at identifying potential hazards within complex systems (Leveson, 2012). The STPA method consists of four main steps. In this section, the derivation of each step is defined based on the formal model and applied to the train-following under NTM-UC.

The **first step** of STPA defines the purpose of the analysis by identifying relevant losses, hazards, and safety constraints, as shown in Table 1. In this study, this identification is grounded in the R2DATO documents (Rail to Digital Automated , 2025), where only Loss L-1 and Hazard H-1 are considered, together with their refined sub-hazards H-1.1 to H-1.3.

Table 1. Selected losses and hazards.

ID	Description	ID Losses
L-1	Loss of life or injury to people on the train	
H-1	Train does not maintain a safe distance to other trains	L-1
H-1.1	Train deceleration is insufficient	
H-1.2	Train deceleration is too late	
H-1.3	Train passes over a point set in the wrong position/direction	

This restriction is motivated by the focus of the formal model on train movement dynamics under NTM-UC. The model does not consider external actors and conditions such as level crossings, people outside the train, or environmental hazards. Sub-hazard H-1.3 slightly differs from the original R2DATO definition, as point behaviour is assumed to be nominal, meaning that points neither provide incorrect indications nor fail to reach their commanded positions.

The **second step** of STPA consists of modelling the system as a control structure that captures the interactions among the components that are responsible for enforcing safety constraints. In this study, the control structure is directly derived from the MB system formal model architecture (Seceleanu et al., 2021), as all relevant elements such as controllers, sensors, controlled processes and communication links are explicitly represented. Figure 2 provides a structure view of the control actions and feedback mechanisms involved in the MB system. It serves as a basis for the subsequent identification of unsafe conditions and CFs in later STPA steps.

After establishing the control structure, the **third step** consists of identifying Unsafe Control Actions (UCAs), which are control actions that can lead to hazards under specific conditions. Formally, in the STPA handbook (Leveson and Thomas, 2018), a UCA is defined as:

$$\text{UCA} = \langle \text{Source} + \text{Type} + \text{Control Action} + \text{Context} + \text{Link to Hazards} \rangle$$

This structured representation ensures that the context in which a control action becomes unsafe

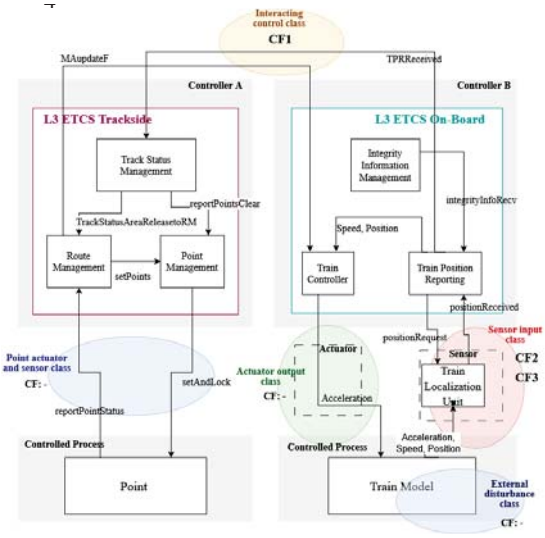

Fig. 2. MB control structure and Causal Factors

is explicitly captured. The UCAs were identified following the four general types of unsafe control actions: (1) not providing the control action leads to a hazard, (2) providing the control action leads to a hazard, (3) providing a potentially safe control action too early, too late, or out of order, and (4) the control action lasts too long or is stopped too soon. Hence, based on the designated control structure in the previous step, the UCAs identified in this study are summarized below:

- UCA-1 (type 1 & type 3): Trackside does not provide or provides MA with delay during NTM-UC following train [H-1.1, H-1.2].
- UCA-2 (type 2): Onboard train controller provides wrong acceleration order during NTM-UC following train [H-1.1, H-1.2].
- UCA-3 (type 2): Moving Block System sets route for a train and moves points while another train occupies the point section [H-1.3].

The **last step** of STPA focuses on identifying loss scenarios, which describe the CFs leading from UCAs to hazards. As pointed out in the STPA handbook, two types of scenarios can be considered: (a) scenarios explaining why unsafe control actions occur, and (b) scenarios where control actions are improperly executed or not executed. In this study, only type (a) scenarios are considered. Type (b) scenarios are addressed through other analyses and fall outside the scope of the technological novelties of the MB system. The following CFs represent possible causes of type (a) loss scenarios identified through the control structure, as shown in Figure 2.

- CF1: The onboard unit does not receive MA or receives the MA command from the Trackside with a delay.
- CF2: The onboard unit receives feedback from sensors with a delay.
- CF3: The onboard unit unit receives erroneous feedback from sensors (measurement inaccuracies).

In the end, based on these CFs, the type (a) loss scenarios for each UCA are defined as follows:

- **Scenario 1:** Communication loss or delay between ETCS trackside and onboard causes the trackside either not to provide the MA or to provide it late [UCA-1], resulting in the train failing to maintain a safe distance to other trains [H-1.1, H-1.2].
- **Scenario 2:** Sensor delay causes the onboard train controller to apply incorrect acceleration while following another train [UCA-2], resulting in unsafe train separation [H-1.1, H-1.2].
- **Scenario 3:** Sensor measurement error causes the onboard train controller to apply incorrect acceleration while following another train [UCA-2], resulting in unsafe train separation [H-1.1, H-1.2].
- **Scenario 4:** Sensor measurement error causes the ETCS trackside to incorrectly assume the point is clear [UCA-3], resulting in a route with a different point position being set while another train occupies the point section [H-1.3].

These loss scenarios establish explicit causal links between UCAs and their underlying causes, providing a structured basis for their formal analysis using model checking techniques.

3.2. *Model Checking Integrated Safety Analysis*

UPPAAL SMC extends UPPAAL with Statistical Model Checking (SMC) facilities to improve

scalability by using simulation based techniques instead of exhaustive state-space exploration. It supports the probabilistic analysis of networks of priced timed automata, enabling the evaluation of time-bounded and probabilistic properties. In this study, UPPAAL SMC is used to analyse the loss scenarios derived from STPA because it supports temporal modelling, modularity, and parametrization, aligns with our prior experience.

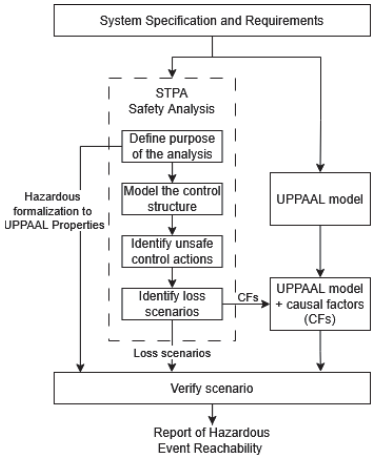

Fig. 3. Integration of STPA and UPPAAL

The integration of STPA and UPPAAL proposed in this work is illustrated in Figure 3. First, it shows how hazardous conditions identified through STPA are formalized as verification safety-related properties in UPPAAL. This formalization is presented in Table 2. Properties P1 and P2 check for train overlap and positions exceeding the authorized limit (MA). If one of these properties is reachable, it implies that hazardous states H-1.1 and H-1.2 can occur. Property P3 checks for unsafe point movement, which implies that H-1.3 can occur. Second, this formalization is used to verify the extended model, into which the CFs derived from STPA are introduced, using SMC.

4. Verification of Loss Scenarios

In this section, the loss scenarios identified through STPA are analysed by introducing CFs derived from STPA into our formal model. The four scenarios identified through STPA are verified using safety-related properties in UPPAAL SMC to examine whether disturbances caused by these CFs can lead to hazardous conditions.

Properties in UPPAAL SMC are specified using queries of the form $\Pr(\varphi)$, which determines the number of simulation runs required to estimate the probability p within an approximation interval $[p-\varepsilon,\ p+\varepsilon]$ with a confidence level of $1-\alpha$, where ε denotes the probability uncertainty and α represents the probability of false negatives. Based on this formulation, probabilistic verification in this paper uses the following query:

$$\mathrm{PR}[LOC\_AbsTime \leq 600](\Diamond(Property))$$

where properties are defined in Table 2.

Table 2. UPPAAL Hazardous Event Formalization

No.	UPPAAL Property	Hazard ID
P1	`<>TS_TSM0.Overlap || TS_TSM1.Overlap || TS_TSM2.Overlap`	[H-1.1, H-1.2]
P2	`<>TS_MA0.Overshoot || TS_MA1.Overshoot || TS_MA2.Overshoot`	[H-1.1, H-1.2]
P3	`<>TS_PM0.PointIncorrect || TS_PM1.PointIncorrect`	[H-1.3]

Before analysing the loss scenarios, we first reverify model correctness behaviour under NTM-UC, i.e. in the absence of CFs. All properties P1, P2, and P3 were found to be unreachable, with an estimated probability of 0 within the considered confidence bounds over 368 simulation runs, which confirms the correctness of the base MB system model logic. Next, we verify the four scenarios. In cases where such verification results show probabilities greater than zero, possible mitigation strategies are also discussed.

In this paper, all UPPAAL SMC parameters are set to $\varepsilon = 0.01$ and $\alpha = 0.05$, with the time frame limited to $600\,\mathrm{s}$, by which time all trains reach a stationary state[a]. All experiments were performed on an Intel Core i7-10610U CPU (4

[a]The UPPAAL models developed for this work can be found at `https://gitlab.univ-eiffel.fr/julie.beugin/ETCS-Moving-Block-System`.

cores, 8 logical processors) with a base frequency of 1.8 GHz.

4.1. *Scenario 1*

To model the communication delay and loss between the ETCS trackside and onboard unit, we refer to (Carnevali et al., 2015). However, since this disturbance is modelled using Petri nets, an equivalent automaton must first be derived. Once obtained, the resulting disturbance model is integrated into our original model. The corresponding communication expiration probabilities are summarized in Table 3 and are consistent with the results reported in the referenced work.

Table 3. Probability of communication expire in UPPAAL Model.

Expire time (s)	Probability (95% CI)	Computing time (s)
12	0.1875 ± 0.0099	1086.702
15	0.0118 ± 0.0097	1524.893
18	0.0072 ± 0.0067	226.783

After implementing the communication error model, safety verification using UPPAAL shows that, despite communication delays and losses between controller A (trackside) and controller B (onboard), the safety of the MB system is not compromised. Specifically, P1 and P2 are not reachable (Table 4), confirming that the MA issued by the trackside always safe with respect to the positions of other trains and the system does not reach hazards H-1.1 and H-1.2.

Table 4. Reachability probabilities of properties under Scenario 1.

Prop. No	Prob. (95% CI)	Occurrence / Nb. Runs	Computing time (s)
P1	≤ 0.0099	$0/368$	86.307
P2	≤ 0.0099	$0/368$	82.289

4.2. *Scenario 2*

To verify this scenario, the causal factor related to sensor delay is explicitly modeled. Instead of using the true train position, the onboard system receives a delayed position measurement. The corresponding automaton model is parameterized, allowing the maximum delay value to be varied during verification.

After the verification process, with results shown in Table 5, the results indicate that measurement delays lead to train position overshoot beyond the permitted area. Although no train overlapping (P1) is observed, the reachability of P2 constitutes a violation of hazard conditions H-1.1 and H-1.2.

Table 5. Reachability probabilities of properties under Scenario 2.

Prop. No	Maximum Delay	Probability (95% CI)	Occurrence / Nb. Runs	Computing time (s)
P1	$30ms$	≤ 0.0099	$0/368$	574.49
	$40ms$	≤ 0.0099	$0/368$	473.736
	$50ms$	≤ 0.0099	$0/368$	619.182
P2	$30ms$	≤ 0.0099	$0/368$	784.749
	$40ms$	$0.6880\pm$ 0.0099	$5815/8451$	10401.83
	$50ms$	$0.9854\pm$ 0.0082	$848/859$	1173.008

To mitigate the impact of delays in the presence of sensor feedback, appropriate controller adjustments can be introduced. A simple mitigation strategy consists in adding a safety margin to the speed supervision control. For example, assuming a maximum GNSS sensor delay of $100\,\mathrm{ms}$, a straightforward calculation shows that such a delay may result in a maximum position overshoot of margin $M = 0.1\,(\mathrm{s}) \cdot V_{\max}\,(\mathrm{m/s})$. When this value M is fully accounted for in the safety margin, the verification of P1 and P2 yields no observed hazardous occurrence.

4.3. *Scenario 3*

For MB operation in ETCS, GNSS can be used, either standalone or in combination with other onboard localisation devices.

In this subsection, the GNSS sensor error data and methodology of sensor fusion are modelled according to (Beugin et al., 2018). First, the GNSS measurement is modelled with errors derived from the reference, reflecting realistic operational performance, as shown in Figure 4. Using this sensor error model, safety verification is performed with

UPPAAL to check whether defined safety properties are reachable.

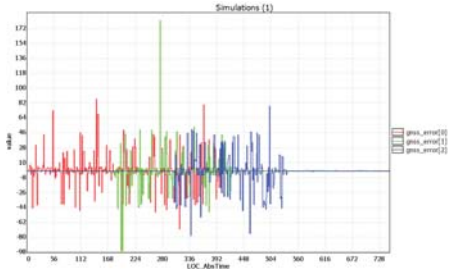

Fig. 4. GNSS error of Trains 0, 1, and 2

In this scenario, the results shown in Table 6 confirm that GNSS-based positioning alone is not sufficiently reliable for MB operation, as overlapping and overshoots consistently occur.

Table 6. Reachability probabilities of properties under Scenario 3.

Prop. No	Prob. (95% CI)	Occurrence / Nb. Runs	Computing time (s)
P1	≥ 0.99	368/368	107.259
P2	≥ 0.99	368/368	76.809

One well-known solution to address this limitation is to use sensor fusion techniques, particularly by combining GNSS measurements with an odometer subject to 5% error of the travelled distance. The odometer is periodically reset by physical trackside balises, reducing measurement errors and improving position accuracy. The analysis in Table 7 shows the reachability probabilities after implementing a simple sensor combination with a Kalman filter, where the odometer sensor is reset every kilometre, in UPPAAL model.

Table 7. Reachability probabilities of properties under Scenario 3 combining GNSS with other sensors.

Prop. No	Prob. (95% CI)	Occurrence / Nb. Runs	Computing time (s)
P1	0.6395 ± 0.01	5778/9035	4039.75
P2	0.1855 ± 0.01	1127/6080	2939.916

Nevertheless, the results show that the probabilities for both safety properties P1 and P2 remain relatively high. This reflects a major challenge in implementing autonomous localisation systems in MB system, which remains an open research problem. The current formal model also does not explicitly represent position uncertainty, such as underestimation and overestimation intervals derived from measurement confidence levels.

4.4. *Scenario 4*

Unlike the sensor delay case, Property P3 may becomes reachable when sensor measurement errors are introduced. In the sensor delay scenario (scenario 2), the train cannot be incorrectly perceived as having already left the point region while it is still occupying it. This is not the case for sensor measurement errors that may cause the perceived train position to deviate from the true position in both directions.

To evaluate reachability of P3 and estimate the associated probabilities, the same GNSS model (with errors) from the previous scenario is first applied. The behaviour of the following train is then simulated under different route-setting times. We consider only two following trains, where the route-setting time for the leading train (Train_0) is fixed at 0 s. In this setting, several route-setting times for the following train (Train_1) may lead to hazardous situations for the leading train, as shown in Table 8, since there is a chance that the point is commanded to move while its zone is still occupied or reserved by the leading train (Train_0). Additionally, finding situation where this hazard occurs is quite tricky, as it requires identifying the suspicious timing set, reducing the simulation uncertainty ε to 10^{-4}, and shortening the time frame to 150 s instead of 600 s, since only the time frame up to when the point moves is relevant rather than the entire simulation until the train stops.

In this Scenario 4, safety again strongly depends on the accuracy of train localisation. An alternative mitigation strategy is to introduce dedicated train detection systems in critical areas, such as point regions. Since points are safety-critical assets, localised detection can provide an additional layer of protection that is independent

Table 8. Reachability probability of property P3 under Scenario 4.

Train_1 setting time (s)	Prob. (95% CI)	Occurrence / Nb. Runs	Computing time (s)
134	$\leq 9.9e^{-5}$	0/36887	3416.974
135	$6.12e^{-5} \pm 6.07e^{-5}$	1/45714	3869.408
136	$6.12e^{-5} \pm 6.07e^{-5}$	1/45714	3749.695
137	$9.97e^{-5} \pm 7.53e^{-5}$	5/66678	5667.463
138	$\leq 9.9e^{-5}$	0/36887	3363.312

of continuous train position estimation.

5. Conclusion and Future Work

In this paper, safety-related operational scenarios that could potentially lead to hazardous events in an ETCS MB system were derived using STPA and analysed using UPPAAL SMC. These scenarios are characterized by casual factors that are explicitly introduced into the formal model. Despite the control-command correctness already proven for NTM-UC in our prior work, the verification results show that some potential hazardous situations are reachable under specific combinations of disturbances and timing conditions, highlighting the relevance of the proposed STPA-driven verification approach for analysing safety-critical behaviour in MB systems. The results also indicate that achieving very small uncertainty levels (e.g., 10^{-4} or 10^{-5}) may require significant computational effort, signifying a trade-off between realistic model checking and computational cost in SMC verification.

As future work, the proposed approach could be extended to more detailed functions such as speed supervision and train position confidence intervals. It could also be implemented in other model checking tools to benchmark the performance of reachability analysis for such complex systems.

Acknowledgement

This research was supported by the "Safety of Railway Systems" Chair funded by CERTIFER.

References

Abdulkhaleq, A. and S. Wagner (2014). Integrated safety analysis using systems-theoretic process analysis and software model checking. In *Computer Safety, Reliability, and Security (SAFECOMP 2014)*, pp. 121–134.

Beugin, J., C. Legrand, J. Marais, M. Berbineau, and E. M. E. Koursi (2018). Safety appraisal of gnss-based localization systems used in train spacing control. *IEEE Access 6*, 9898–9916.

Carnevali, L., F. Flammini, M. Paolieri, and E. Vicario (2015). Non-markovian performability evaluation of ertms/etcs level 3. In M. Beltrán et al. (Eds.), *Computer Performance Engineering*, Volume 9272 of *Lecture Notes in Computer Science*, Cham, pp. 47–62. Springer.

David, A., K. G. Larsen, A. Legay, M. Mikučionis, and D. B. Poulsen (2015). UPPAAL SMC tutorial. *International Journal on Software Tools for Technology Transfer 17*(4), 397–415.

Leveson, N. G. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press.

Leveson, N. G. and J. P. Thomas (2018). *STPA Handbook*. N. Leveson.

Pakonen, A., I. Buzhinsky, and K. Björkman (2021). Model checking reveals design issues leading to spurious actuation of nuclear instrumentation and control systems. *Reliability Engineering and System Safety 205*, 107237.

Rail to Digital Automated (2025). D13.1 – moving block specifications, part 3 – safety analysis. Technical report, ÖBB-INFRA. Project funded by the European Union's Horizon Europe programme.

Recta, A., R. Saddem-Yagoubi, J. Beugin, and M. Ghazel (2025). Formal modeling and verification of advanced railway route management with moving blocks. In *Proceedings of the International Conference on System Reliability and Safety (ICSRS)*. IEEE. To appear.

Seceleanu et al. (2021). Deliverable d2.1: Modelling guidelines and moving block use cases characterization. Project Deliverable D2.1, PERFORMINGRAIL EU Project.

Tsuji, M., T. Takai, K. Kakimoto, N. Ishihama, M. Katahira, and H. Iida (2020). Prioritizing scenarios based on stamp/stpa using statistical model checking. In *Proceedings of the IEEE International Conference on Software Testing Workshops (ICSTW)*. IEEE.

X2Rail-5 (2022). D4.1 – moving block specification, part 6 – safety analysis. Technical report, Shift2Rail EU Project.

Zhang, Y. and S. Liu (2018). Stpa based safety analysis of regional data center in ctcs-1 train control system. In *Proceedings of the IEEE International Conference of Safety Produce Informatization (IICSPI)*. IEEE.