Formal Methods for Industrial Critical Systems
30 Years of Railway Applications

Maurice H. ter Beek[1], Alessandro Fantechi[1,2], and Stefania Gnesi[1(✉)]

[1] Formal Methods and Tools Lab, CNR–ISTI, Pisa, Italy
{maurice.terbeek,stefania.gnesi}@isti.cnr.it
[2] University of Florence, Florence, Italy
alessandro.fantechi@unifi.it

Abstract. This paper, written in honour of Tiziana Margaria, aims to provide a comprehensive presentation of where mainstream formal methods are currently used for modelling and analysis of railway applications.

1 Introduction

Our collaboration with Tiziana Margaria has a long history, which is part of the history of the Working Group on Formal Methods for Industrial Critical Systems (FMICS)[1] of the European Research Consortium for Informatics and Mathematics (ERCIM)[2], the oldest active working group in this consortium. The FMICS WG, founded in 1996, focuses on the development of formal verification techniques and leads activities, such as joint international projects, related to verification and other formal aspects of software, with a keen eye to industrial applicability. The authors share with Tiziana that they have all chaired this WG.

The annual FMICS conference, first organised in 1996, has held its 29th edition in September 2024. Tiziana chaired the 2005 edition of this conference series [73], whose proceedings are published by Springer in its LNCS series since 2006 (cf., e.g., [14,17,28]), while special issues with extended version of selected conference contributions have regularly appeared in prestigious formal methods journals (cf., e.g., [30,52,54–56,74]; for many years now, these special issues are published in the *International Journal on Software Tools for Technology Transfer* (cf., e.g., [15,16,42]), of which Tiziana is Coordinating Editor and Editor-in-Chief of the thematic theme Foundations for Mastering Change (FoMaC).

The activities of the FMICS WG have stimulated an ongoing scientific discussion on identifying the most efficient formal development and verification techniques, with industrial applicability in mind. Most members of the FMICS community have strong links with the industry and have thus directly contributed to

The original version of the chapter has been revised. The author list in reference 51 been corrected. A correction to this chapter can be found at https://doi.org/10.1007/978-3-031-73887-6_24

[1] https://fmics.inria.fr.

[2] https://www.ercim.eu.

M. Hinchey and B. Steffen (Eds.): Festschrift Tiziana Margaria, LNCS 15240, pp. 327–344, 2025.
https://doi.org/10.1007/978-3-031-73887-6_21

the slow but constant introduction of formal methods in the development cycle of industrial critical systems witnessed during the last decades [13,71].

In 2013, as a follow-up of an FMICS workshop held in Aix-les-Bains in 2004, Tiziana and Stefania edited a book [57] (cf. Fig. 1) to provide a comprehensive presentation of the mainstream formal methods that were used at that time for designing industrial critical systems. The purpose of this book was threefold: (i) to reduce the learning effort of formal methods, which is typically seen as a major drawback for their industrial dissemination; (ii) to help designers adopt the formal methods that are most appropriate for their systems; and (iii) to offer state-of-the-art techniques and tools for analyzing critical systems. All authors contributed to this book. Tiziana has also been involved in other joint efforts by FMICS members [4,66,72,75].

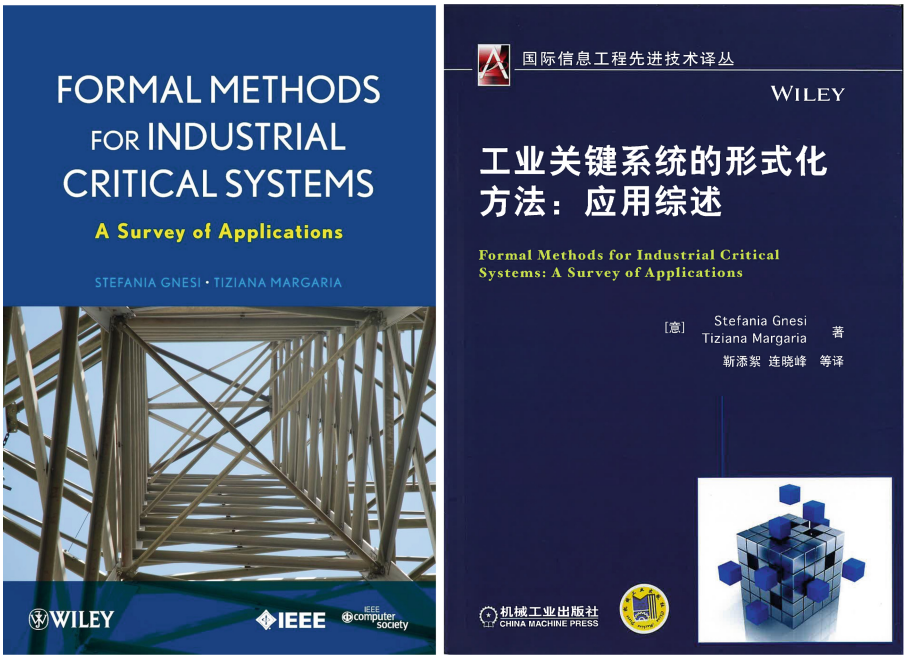

Fig. 1. Covers of the FMICS Working Group book [57] edited by Tiziana and Stefania

Nowadays, the necessity of formal methods as an essential step in the design process of industrial safety-critical systems is widely recognized. In its more general definition, the term *formal methods* encompasses all notations that have a precise mathematical semantics, together with their associated analysis tools, and which describe the behavior of a system in a formal manner [51]. Many formal methods have emerged during the last few decades. Although the benefits of using these formal methods are undeniable, practical experience shows that each particular method is suitable for handling specific aspects of a system. Therefore, the design of a complex industrial system ideally requires expertise in several formal methods to describe and analyze different views of the system.

Successful applications of formal methods in industry (in particular in the transport domain) have demonstrated these benefits to varying degrees, and have shown that the number of defects in the code can be significantly reduced [13,33]. However, formal methods as yet do not pervade the critical software industry, and this happens also in the railway domain, that is by far the domain in which, for several decades now, most success stories have been reported [10,11,39,40,46,49]. These success stories are also due to the fact that formal methods are highly recommended by the CENELEC standards [38] for the development of the most critical software for use in the railway industry.

The high expectations concerning safety, but also concerning availability and performance, of advanced future computer-based railway signalling systems, which are large geographically distributed computing systems, can only be successfully addressed by a systematic adoption of formal methods in their definition and development [43,44,80]. This view has been shared by numerous projects within the Shift2Rail Joint Undertaking (JU) such as X2Rail, ASTRail, 4SECURail, PerformingRail, etc.[3] (more below in Sect. 2.4). Although it is not possible to exhaustively cite the success stories of formal methods adoption in railways here, we refer to the vast literature on the theme through some relevant surveys that have recently been published [6,11,46,47].

This paper aims to provide a comprehensive presentation of where mainstream formal methods are currently used for designing railway applications, as well as pointers for their application to future railways systems.

2 Survey on Railway Systems and Related Applications of Formal Methods

Modern railways are in most cases controlled by real-time computer-based systems. Those systems feature embedded, cyber-physical, distributed and heterogeneous architectures, which are increasingly large and complex. To fulfil the safety requirements, railway control systems must undergo extensive verification and validation, which is typically rather time-consuming when conducted by intensive software testing. Model-based analyses and formal methods promise to make such verification activities less error-prone, therefore increasing the effectiveness and efficiency of the overall process.

The main safety-critical railway signalling equipment can roughly be classified in two large classes of applications, excluding just a few future innovations:

1. train movement and distancing control systems, including three subsystems:
   ATC – Automatic Train Control
   ATP – Automatic Train Protection
   ATO – Automatic Train Operation
2. **IXL** – interlocking (Input and eXit Locking) systems
3. other equipment and future advancements

[3] https://projects.shift2rail.org/s2r_projects.aspx.

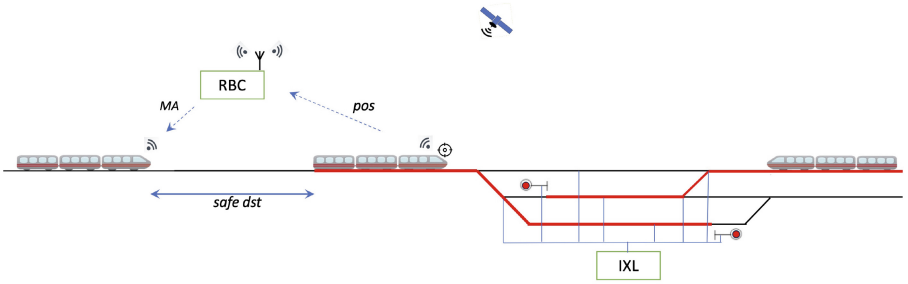

Fig. 2. Main classes of railway signalling systems

Figure 2 provides a broad outline of the purpose of the two classes. On the left, it showcases a train control system based on the communication between trains and a central controller—a so-called Radio Block Centre (RBC), according to ETCS terminology. On the right, it showcases an IXL system controlling the routing of trains inside a station. The drawing also hints at future innovations, among which the use of GPS/GNSS-based satellite positioning of trains [7,70].

2.1 Automatic Train Control and Other Subsystems

ATC subsystems are complex *systems of systems*, made of distributed equipment located on the ground (a.k.a. wayside or trackside) and on board the trains. The main objective of the on-board ATC subsystem is to elaborate and apply the so-called 'dynamic speed profile' (a.k.a. *braking curve*) to control the maximum train speed and automatically brake in case of need (i.e., in case of a risk of collision). To this aim, the on-board ATC subsystem receives the necessary information on the allowed maximum speed and on the status of the line from trackside subsystems: in current ATC subsystems, trains typically receive *Movement Authority* (MA) messages via radio from a monitoring centre that computes related information based on knowledge of the position of the trains along the line. The safety-critical enforcement of emergency braking is also called Automatic Train Protection (ATP).

Modern driverless ATC subsystems have Automatic Train Operation (ATO) functionalities, often used in metro railways, allowing the train to automatically accelerate and decelerate to respect the speed profile and even stop in stations for passenger service whenever required. ATC subsystems may also feature auxiliary control functionalities (e.g., control of pantographs, train integrity check).

The main representatives of ATC/ATP/ATO subsystems respect international standards to ensure interoperability between the different subsystems described. These include ERTMS/ETCS (European Rail Traffic Management Systems/European Train Control System), its Chinese counterpart CTCS (Chinese Train Control System), both focusing on interoperability for passenger, high speed and freight lines, and CBTC (Communication-Based Train Control) systems, mainly aimed at the automatic operation of high capacity metro lines.

The main characteristic of CBTC, shared with ERTMS/ETCS level 3, is the concept of *moving block* signalling (more below in Sect. 2.3). In a nutshell, it consists of computing the safety distance between trains by considering the exact position of each train rather than considering the segment of the line occupied by the train as its position. The wayside ATP for CBTC systems is typically called Zone Controller.

These classes of subsystems have been subject to formal specification and verification for several decades now, as witnessed by the success stories of the application of the B method to many cases, which include the verification of the ATP system for the RER Line A of Paris [59], the Subway Speed Control System (SSCS) of the subway of Calcutta [32], and Line 14 of the Paris Metro [35], as well as derivatives thereof, like line 1 or the NY Canarsie line [37], or the driverless Paris–Roissy Airport shuttle [18]; B was also used for an industrial scale analysis of Alstom's U400 system [29], which is in operation in about 100 metro lines worldwide. Further success stories of applications of formal methods include the metro control system of Rio de Janeiro, with the support of Simulink/Stateflow [48], ERTMS/ETCS with NuSMV [26] and, in [2], the MA scenario of CTCS level 3 modelled in the Architectural Analysis and Design Language (AADL) and in Hybrid CSP and verified with the Hybrid Hoare Logic (HHL) Prover based on Isabelle/HOL.

2.2 Interlocking Systems

A railway *interlocking* (IXL) system is responsible for guiding trains safely through a given railway network made of track devices such as junctions and crossings, providing exclusive access to the requested routes. Once a route is set for a train, all movable devices belonging to the route are set in a locked position and a signal to proceed over that route is given; when the train has passed beyond the section of the track involved, the section and the route are released for successive reservations by other trains. The IXL safety logic is mostly realised through control tables, a set of rules/constraints that must be observed and that are an abstract specification for the area under the IXL responsibility. The IXL control tables are designed such that it is impossible to display a signal to proceed unless the route to be used is proven safe. In this way, no other train is allowed to enter a conflicting route until it is released by the IXL system.

The equation-based tabular nature of the IXL systems, and the fact that their safety requirements can easily be expressed in temporal logic, makes them particularly amenable for formal verification employing model checking or SMT solving. However, these verification tasks share the combinatorial state-space explosion problem, due to the high number of Boolean variables involved, especially in the case of IXL systems controlling large stations: the first applications of model checking, tracing back to the late nineties, have addressed portions of an IXL system (cf., e.g., [20,27,58]); later studies have benefited from the more powerful verification engines powered by SMT solvers [22,64], and focused on the use of specific abstractions [21,65] or of compositional reasoning [61,68] to address the state-space explosion problem.

2.3 Other Equipment and Future Advancements

The classification presented in the beginning of this section excludes a number of other railway equipment that has nevertheless captured the interest of the formal methods community due to the high degree of responsibility for software to ensure safety. These include safety-critical systems that are ancillary to the previous ones (such as the control of level crossings or platform screen doors), systems focused on traffic management/supervision, or envisioned future advances in train control policies. We mention some of these systems in this section.

Level Crossings. Level crossing control has been used as a case study in several studies on the use of formal methods in railways, due to the high safety concerns generated by the intersection of road and rail traffic. A notable example is the use of validation of model checking with UPPAAL of a novel design of a level crossing protection system [53].

Platform Screen Doors. In automated metros, typically operating in a closed environment, platform screen doors are adopted to avoid users to enter or to fall on the tracks. A platform screen door controller has the responsibility of opening only when the train's doors are perfectly aligned with the platform doors. It is worth mentioning that the software of several such installations around the world was developed with the help of the B method [67].

ATS (Automatic Train Supervision). ATS systems aim to supervision the railway system for all those high-level monitoring, track optimisation and maintenance operations not addressed by the other subsystems. While many tasks related to ATS systems (e.g., remote route lock/unlock command) cannot be considered as safety critical since other subsystems will provide the necessary protection against hazards, there are situations in which a certain level of criticality is assigned to those systems as well, for instance when they can be used to activate rescue interventions in case of anomalies requiring feedback from train operators. An ATS system typically acts by issuing route requests to an IXL system; doing so, it can easily incur in deadlocks due to the IXL constraints. Deadlock avoidance can be tackled by model checking, as shown in [76,77].

Moving Block. The ERTMS/ETCS standard considers different levels of operation for compliant ATC systems. In the most advanced one, ERTMS/ETCS level 3, there are no track occupancy sensors and it is the responsibility of an on-board odometry system to keep track of the train's position, as well as to compute the current train speed. The on-board computer of each train periodically sends to the RBC a position report and the results of a train integrity check. In turn, the RBC sends the MA back to each train. The MA is computed by considering the minimum safe rear end of the foregoing train (*moving block* signalling), further improving a line's throughput and reducing maintenance costs.

The absence of track circuits as safe train detection and localisation mechanism, and the difficulty of computing the exact train position, have so far prevented the actual deployment of ETCS level 3 systems, due to safety concerns.

Nevertheless, ETCS level 3 is currently the most promising level of operation in terms of safety increase, capacity gains and maintenance cost reduction. As such it provides a challenging case study; in particular, there is a rich literature on the application of a variety of formal methods and tools to a downsized version named ERTMS/ETCS Hybrid L3 [1,3,5,7,24,31,34,60,69,81].

Satellite Positioning. The localisation of trains along a line is currently detected by specific trackside sensors (such as track circuits or axle counters) that are able to detect the occupancy of a track section. More precise computation of the current position of a train, required by moving block signalling systems, can be achieved by on-board odometry, accelerometers and other sensors. Satellite positioning promises to become an absolute positioning system, significantly reducing the need and cost of trackside sensing equipment. The statistical nature of positioning information given by GPS/GNSS sensors requires a paradigm shift from qualitative formal verification of safety towards quantitative evaluation aimed at the validation of probabilistic safety requirements. In this regard, UPPAAL's statistical model-checking features were considered in [62,63] for the evaluation of GNSS localisation in the context of ETCS level 3.

The same choice was followed for the safety verification of the satellite-based Autonomous Positioning System (APS) of the Florence tramways in [9].

Virtual Coupling. Further challenges arise from visionary advances of the moving block concept. Indeed, the availability of safe information concerning the position, speed, acceleration and deceleration of the preceding train, like that used in level 3 of ERTMS/ETCS, has inspired the idea of an innovative method of train formation, called Virtual Coupling (VC). The concept, which resembles the platooning concept studied in the automotive domain, is based on the idea of multiple trains that run one behind the other without physical contact but at a distance comparable to mechanical coupling. The strict real-time control of the dynamic parameters of the following train with respect to those of the preceding train, allows the distance between trains to be minimised, thus allowing high flexibility, for instance in forwarding the different segments of a train to different destinations through composition and decomposition during the run. Notably, VC is one of the challenges addressed in the Multiannual Programme of the Shift2Rail JU Initiative and its potential has been studied in [50,78] in the context of the Shift2Rail project PERFORMINGRAIL (more below in Sect. 2.4).

Standard Interfaces. When all subsystems described above, which are typically validated separately, interact with each other—as is the case in all modern settings—it becomes essential to also validate the interfaces between these subsystems. The reason is that some hazards might possibly be generated at the inter-communication protocol level. Formal methods are among the methods specifically adopted for this purpose (cf., e.g., [8,19]), since they are suitable

to detect anomalies in the specification and implementation of communication protocols.

2.4 International Projects on Formal Methods and Railways

With no claim to completeness, we briefly describe some international projects on applying formal methods in the railway domain.

EuroInterlocking This project of the International Union of Railways (UIC) aimed at the harmonisation, joint development, and standardisation of IXL and signalling systems in Europe. In particular, it has contributed to the development of standardised file formats for IXL data exchange, and to the construction of a generic simulation tool (exploiting the project-defined location and IXL file formats) for the verification and validation of IXL rules.

EuRailCheck[4] (European Railway Formalization and Validation): This was a project of the European Railway Agency (ERA). The objective of this project was the development of a methodology and supporting tools for the formalisation and validation of (a subset of) the ETCS specifications. Within the project, three main results were achieved: a methodology for the formalisation and validation of the ETCS specifications that goes from the informal analysis of the requirements to their formalisation and validation; a set of support tools, covering the various phases of the methodology; and a realistic subset of the formalised specifications.

INESS[5] (INtegrated European Signalling System): The main goal of this EU FP7 project was to extend and enhance the standardisation process defining and developing specifications for a new generation of IXL systems. One of its tasks was to identify safety requirements of the IXL model and their representation in a formal format, as invariant state properties (using UML-B). A prototypical tool for the verification of these invariants was developed.

EULYNX[6] (European Initiative Linking Interlocking Subsystems): This was an initiative of European Infrastructure Managers. The project aspired to a mutually shared vision toward harmonisation of railway signalling systems, their technical architecture, functions and interfaces. The project includes items like system architecture, modelling and testing, data preparation, interfaces between IXL systems, interfaces to track vacancy detection and adjacent IXL or signalling subsystems: requirement management tools, UML (Unified Modelling Language) and SysML (Systems Modelling Language) modelling techniques were used to formalise unambiguous requirements.

ASTRail[7] (SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block validation): This EU H2020 Shift2Rail project included (i) an analysis phase, dedicated to the comparison and evaluation of the main formal methods and tools that were being

[4] https://es-static.fbk.eu/projects/eurailcheck/.
[5] https://www.iness.eu.
[6] https://eulynx.eu.
[7] http://www.astrail.eu.

used at that time in the railway industry to guarantee that software design and implementation criticalities do not jeopardise the safety, as well as (ii) an application phase, in which selected formal methods were used to model and analyse two main goals addressed by the project, namely moving block distancing and automatic driving. The aim was to validate that the formal methods are not only able to guarantee safety issues, but also—more in general—the long term reliability and availability of the software.

X2RAIL-2[8] (Enhancing Railway Signaling Systems): This EU H2020 Shift2-Rail project carried out a survey to identify the railway signalling industry's expectations of formal methods and tools, in terms of their most important characteristics, benefits and challenges. This survey [83] showed that formal methods can provide significant benefits to railway signalling system development in terms of improved safety, better requirement quality and reliability and, finally, reduced time-to-market and cost. However, the survey indicated that there are also significant obstacles increasing to the widespread use of formal methods to gain such benefits. The main obstacle is the high learning curve and indeed formal methods have the image of being too difficult to apply for "ordinary engineers". This survey moreover showed that the use of formal methods would be helped by more standardised interfaces.

4SECURail[9] (FORmal Methods and CSIRT for the RAILway sector): This EU H2020 Shift2Rail project addressed the development of a demonstrator for the use of formal methods in the railway environment. This project provided a demonstrator of state-of-the-art formal methods and tools to evaluate the learning curve and to perform a cost-benefit analysis of the adoption of formal methods in the railway industry. The demonstrator has been applied to a railway signalling subsystem described using standard interfaces aimed at illustrating some usable state-of-the-art techniques for rigorous standard interface specification, as well as at supporting a cost-benefit analysis to back this strategy with sound economic arguments.

PERFORMINGRAIL[10] (PERformance-based Formal modelling and Optimal tRaffic Management for movING-block RAILway signalling): This EU H2020 Shift2Rail project aimed to deliver formal modelling and optimal traffic management of a moving block railway signalling system using advanced train positioning approaches that mitigate potential hazards in the diverse market segments. It implemented a holistic system approach to address the open challenges for the moving block and VC concepts in terms of safe operational principles and specifications, reliable TIM technologies, high-accuracy train localisation and optimised moving block traffic management algorithms. The main objectives were to enhance and verify existing specifications for moving block signalling, while developing formal models, algorithms and proof-of-concepts to test and validate an integrated future mov-

[8] https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-2.
[9] http://www.4securail.eu.
[10] https://www.performingrail.com.

ing block system architecture that will provide safe and effective operational performance.

X2RAIL-5[11] (Advanced Traffic Management & Control Systems): This EU H2020 Shift2Rail project had the objective to improve the standardisation and integration of formal methods application in the development of Europe's rail control systems while reducing time to market and improving effectiveness in the introduction of new signalling and supervision systems. A particular project output was to propose and apply a methodology and toolchain to automate the transformation of semi-formal (specification) models into models suitable for formal verification. The objective was to create a tool that can automatically translate the semi-formal SysML models into a formal model, to obtain a more precise and rigorous representation of the system, and to apply formal verification to prove properties against the formal model. According to this, two toolchains were proposed for the automated transformation of EULYNX SysML models into formal models.

3 ISoLA: Leveraging Applications of Formal Methods, Verification and Validation

ISoLA is a highly successful symposium series[12], currently at its 12th edition, for developers, users and researchers to discuss issues related to the adoption and use of rigorous tools, based on formal methods, for the specification, analysis, verification, certification, construction, testing and maintenance of systems from the perspective of their different application domains, instituted by Tiziana and Bernhard Steffen.

The adoption of formal methods in railway signalling has been the subject of specific tracks at ISoLA conferences for over a decade now. The "Formal Methods for Intelligent Transportation Systems" track, held at ISoLA 2012 [41], focused on railway applications, as a recognition of how much the railway signalling sector has been a source of success stories on the adoption of formal methods. The "Formal Methods and Safety Certification: Challenges in the Railways Domain" track, held at ISoLA 2016 [40], addressed the many challenges posed by the increasing scale and complexity of railway systems.

In 2019, a workshop colocated with the DisCoTec federated conference on distributed computing techniques, coined DisCoRail ("Formal methods for DIStributed COmputing in future RAILway systems"), was initiated. The aim of this workshop series is to discuss how distributed computing is affecting the railway signalling domain, given that the new technologies being applied in this domain (with a main example represented by the wide deployment of ERTMS/ETCS systems on high-speed lines as well as on freight corridors) have transformed railways in a very large geographic distributed computing system.

It thus appeared evident that the high expectations on safety, but also on availability and performance of future railway signalling systems, in the presence

[11] https://verkehrsforschung.dlr.de/en/projects/x2rail-5.
[12] https://www.isola-conference.org.

of a high degree of distribution, can only be addressed by the systematic adoption of formal methods in the definition and development of such systems. This view was shared by several projects within the Shift2Rail JU, which were represented in the successive editions of the DisCoRail workshop, held at ISoLA 2020/21 [43] as a track on "Formal methods for DIStributed COmputing in future RAILway systems", replicated at the ISoLA 2022 and 2024 editions [44,45].

4 Conclusion

The use of formal methods and tools is an essential step in the design process of industrial safety-critical systems. Their successful application in the transport domain has demonstrated several benefits, showing that the number of defects in the code can be significantly reduced. The aim of this paper is to provide a comprehensive presentation of where mainstream formal methods are currently being used for designing railway applications, as well as future advanced railway systems where their application might turn out useful. Yet there are significant obstacles that hinder a greater use of formal methods to achieve benefits.

Presumably the greatest obstacle is the steep learning curve. A recent survey among 130 experts in formal methods (including—next to Tiziana—3 Turing Award winners[13], all 5 FME Fellowship Award winners[14], 17 CAV Award winners[15]) investigated the factors limiting the uptake of formal methods in industry [51, Section 5: Formal Methods in Industry]. These experts recognised several limiting factors: "academic tools have limitations and are not professionally maintained" (66.9%), formal methods "are not properly integrated in the industrial design life cycle" (66.9%) and "have a steep learning curve" (63.8%). Moreover, 62.3% of the respondents indicated that "developers are reluctant to change their way of working." Alas, formal methods have the image of being too difficult. Yet, according to this expert survey, the key *limiting factor for a wider adoption of formal methods by industry*, identified by 71.5% of the respondents, is that "engineers lack proper training in formal methods".

This conclusion is shared by numerous experts. A recent white paper [25], which presents the outcome of a Workshop on Formal Methods, advocates "the inclusion of a compulsory formal methods course in Computer Science (CS) and software engineering curricula" based on the observation that "there is a lack of CS graduates who are qualified to apply formal methods in industry".

In the context of safety- and mission-critical applications, a very recent paper recognises "an urgent need to emphasize and integrate formal methods into the undergraduate curriculum in CS in the United States", since "the lack of a well-structured exposure to formal methods is a serious shortcoming in our computing curricula" [79]: "We cannot expect graduates to become experts in program verification as professionals if they never encountered the ideas as students".

[13] https://amturing.acm.org/byyear.cfm.
[14] https://www.fmeurope.org/awards/.
[15] http://i-cav.org/cav-award/.

Finally, [12] advocates a prominent role of formal methods in the ACM/IEEE-CS/AAAI CS2023 curriculum and provides concrete suggestions for educators to incorporate formal methods into CS education without displacing other engineering aspects of CS that are already widely accepted as essential. This paper is based on three accompanying papers which underline (i) the importance of formal methods *thinking* in CS education [36], since it provides the necessary rigour in reasoning about correctness which is a fundamental skill for future software developers; (ii) that every computer scientist needs to *know* formal methods [23], since the skills and knowledge acquired from studying formal methods provide the indispensable solid foundation that forms the backbone of CS practice; and (iii) the increasing *use* of formal methods in industry [13], not limited to safety-critical domain, which demonstrates that formal methods have wide-ranging practical value in a in a society that increasingly relies on software.

Other significant obstacles to further adoption of formal methods in the railway domain include the fact that applicable standards (such as CENELEC EN 50128 [38]) are not sufficiently clear on how to actually use formal methods cost-effectively and the lack of a clear picture of what can be achieved by using formal methods (in terms of benefits, both technical and economical; even though a recent study reports promising cost savings [19, Section 3: Cost-Benefit Analysis]. This leads management to deem formal methods too risky. The aforementioned survey among 130 experts in formal methods also contained a question that asked the respondents to make an informal cost-benefit analysis over time [51, Section 5.3: Return on Investment]. A small majority of 58.5% of the respondents answered that the application of formal methods is *profitable in medium and long terms*; 15% that they are *immediately profitable* and 12.3% answered that they are *profitable in the long term only*, while 2.3% answered that there is *no return on investment* and 11.5% had *no opinion*.

Another obstacle to the widespread use of formal methods is the current lack of commercial formal tools, easy to integrate in the software development process and working on open standard formats [49]. The state-of-the-art of the development tools market apparently sees either the offer of industry-ready, well-maintained, and supported tools working on closed proprietary formats, or open-source tools working on standard open format but offering a low level of support and maintenance.

But the future is bright! The formal methods community recently received support from The White House [82, Part II: Securing the Building Blocks of Cyberspace—Formal Methods]: "Given the complexities of code, testing is a necessary but insufficient step in the development process to fully reduce vulnerabilities at scale. If correctness is defined as the ability of a piece of software to meet a specific security requirement, then it is possible to demonstrate correctness using mathematical techniques called *formal methods*. [...] While formal methods have been studied for decades, their deployment remains limited; further innovation in approaches to make formal methods widely accessible is vital to accelerate broad adoption."

Acknowledgements. This paper is dedicated to Tiziana Margaria to celebrate her diamond jubilee (never mention a lady's age!). While none of us ever wrote a paper with Tiziana, we all have many fond memories of meetings (in particular within the FMICS WG), dinners (never in Italian restaurants outside Italy!) and conferences (in particular at the *ευήλιοζ* ISoLA series, *the place* for networking on formal methods!). *Buon compleanno, Tiziana!*

Part of this study was carried out within the MUR PRIN 2022 PNRR P2022A492B project ADVENTURE (ADVancEd iNtegraTed evalUation of Railway systEms) and the MOST – Sustainable Mobility National Research Center and received funding from the European Union NextGenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4, COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023. This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them.

Conflicts of interest. The author(s) has no competing interests to declare that are relevant to the content of this manuscript.

References

1. Abrial, J.: The ABZ-2018 case study with Event-B. Int. J. Softw. Tools Technol. Transf. **22**(3), 257–264 (2020). https://doi.org/10.1007/s10009-019-00525-3
2. Ahmad, E., Dong, Y., Larson, B.R., Lü, J., Tang, T., Zhan, N.: Behavior modeling and verification of movement authority scenario of Chinese train control system using AADL. Sci. China Inf. Sci. **58**(11), 1–20 (2015). https://doi.org/10.1007/s11432-015-5346-2
3. Arcaini, P., Kofroň, J., Ježek, P.: Validation of the hybrid ERTMS/ETCS level 3 using SPIN. Int. J. Softw. Tools Technol. Transf. **22**(3), 265–279 (2020). https://doi.org/10.1007/s10009-019-00539-x
4. Arenas, A.E., Bicarregui, J., Margaria, T.: The FMICS view on the verified software repository. J. Integr. Des. Process. Sci. **10**(4), 47–54 (2006)
5. Bartholomeus, M., Luttik, B., Willemse, T.: Modelling and analysing ERTMS hybrid level 3 with the mCRL2 toolset. In: Howar, F., Barnat, J. (eds.) FMICS 2018. LNCS, vol. 11119, pp. 98–114. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00244-2_7
6. Basile, D., et al.: On the industrial uptake of formal methods in the railway domain. In: Furia, C.A., Winter, K. (eds.) IFM 2018. LNCS, vol. 11023, pp. 20–29. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98938-9_2
7. Basile, D., ter Beek, M.H., Ferrari, A., Legay, A.: Exploring the ERTMS/ETCS full moving block specification: an experience with formal methods. Int. J. Softw. Tools Technol. Transf. **24**(3), 351–370 (2022). https://doi.org/10.1007/s10009-022-00653-3
8. Basile, D., Fantechi, A., Rosadi, I.: Formal analysis of the UNISIG safety application intermediate sub-layer. In: Lluch Lafuente, A., Mavridou, A. (eds.) FMICS 2021. LNCS, vol. 12863, pp. 174–190. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-85248-1_11
9. Basile, D., Fantechi, A., Rucher, L., Mandò, G.: Analysing an autonomous tramway positioning system with the Uppaal statistical model checker. Form. Asp. Comput. **33**(6), 957–987 (2021). https://doi.org/10.1007/s00165-021-00556-1

10. ter Beek, M.H.: Formal methods and tools applied in the railway domain. In: Bonfanti, S., Gargantini, A., Leuschel, M., Riccobene, E., Scandurra, P. (eds.) ABZ 2024. LNCS, vol. 14759, pp. 3–21. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-63790-2_1
11. ter Beek, M.H., et al.: Adopting formal methods in an industrial setting: the railways case. In: ter Beek, M.H., McIver, A., Oliveira, J.N. (eds.) FM 2019. LNCS, vol. 11800, pp. 762–772. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30942-8_46
12. ter Beek, M., Broy, M., Dongol, B.: The role of formal methods in computer science education. ACM InRoads **15**(4), 58–66 (2024). https://doi.org/10.1145/3702231
13. ter Beek, M.H., et al.: Formal methods in industry. Form. Asp. Comput. **37**(1), 7:1-7:38 (2025). https://doi.org/10.1145/3689374
14. ter Beek, M.H., Gnesi, S., Knapp, A. (eds.): FMICS/AVoCS 2016. LNCS, vol. 9933. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45943-1
15. ter Beek, M.H., Gnesi, S., Knapp, A.: Formal methods and automated verification of critical systems. Int. J. Softw. Tools Technol. Transf. **20**(4), 355–358 (2018). https://doi.org/10.1007/s10009-018-0494-5
16. ter Beek, M.H., Gnesi, S., Knapp, A.: Formal methods for transport systems. Int. J. Softw. Tools Technol. Transf. **20**(3), 237–241 (2018). https://doi.org/10.1007/s10009-018-0487-4
17. ter Beek, M.H., Ničković, D. (eds.): FMICS 2020. LNCS, vol. 12327. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58298-2
18. Behm, P., Benoit, P., Faivre, A., Meynadier, J.-M.: Météor: a successful application of B in a large project. In: Wing, J.M., Woodcock, J., Davies, J. (eds.) FM 1999. LNCS, vol. 1708, pp. 369–387. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48119-2_22
19. Belli, D., et al.: The 4SECURail case study on rigorous standard interface specifications. In: Cimatti, A., Titolo, L. (eds.) FMICS 2023. LNCS, vol. 14290, pp. 22–39. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-43681-9_2
20. Bernardeschi, C., Fantechi, A., Gnesi, S., Larosa, S., Mongardi, G., Romano, D.: A formal verification environment for railway signaling system design. Form. Methods Syst. Des. **12**(2), 139–161 (1998). https://doi.org/10.1023/A:1008645826258
21. Bonacchi, A., Fantechi, A., Bacherini, S., Tempestini, M.: Validation process for railway interlocking systems. Sci. Comput. Program. **128**, 2–21 (2016). https://doi.org/10.1016/j.scico.2016.04.004
22. Borälv, A.: Interlocking design automation using Prover Trident. In: Havelund, K., Peleska, J., Roscoe, B., de Vink, E. (eds.) FM 2018. LNCS, vol. 10951, pp. 653–656. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-95582-7_39
23. Broy, M., et al.: Does every computer scientist need to know formal methods? Form. Asp. Comput. (2024). https://doi.org/10.1145/36707
24. Butler, M., Hoang, T.S., Raschke, A., Reichl, K.: Introduction to special section on the ABZ 2018 case study: hybrid ERTMS/ETCS Level 3. Int. J. Softw. Tools Technol. Transf. **22**(3), 249–255 (2020). https://doi.org/10.1007/s10009-020-00562-3
25. Cerone, A., et al.: Rooting formal methods within higher education curricula for computer science and software engineering — a white paper —. In: Cerone, A., Roggenbach, M. (eds.) FMFun 2019. CCIS, vol. 1301, pp. 1–26. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-71374-4_1
26. Chiappini, A., et al.: Formalization and validation of a subset of the European Train Control System. In: ICSE 2010, pp. 109–118. ACM (2010). https://doi.org/10.1145/1810295.1810312

27. Cimatti, A., Giunchiglia, F., Mongardi, G., Romano, D., Torielli, F., Traverso, P.: Formal verification of a railway interlocking system using model checking. Form. Asp. Comput. **10**(4), 361–380 (1998). https://doi.org/10.1007/S001650050022
28. Cofer, D., Fantechi, A. (eds.): FMICS 2008. LNCS, vol. 5596. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03240-0
29. Comptier, M., Leuschel, M., Mejia, L.-F., Perez, J.M., Mutz, M.: Property-based modelling and validation of a CBTC zone controller in Event-B. In: Collart-Dutilleul, S., Lecomte, T., Romanovsky, A. (eds.) RSSRail 2019. LNCS, vol. 11495, pp. 202–212. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-18744-6_13
30. Cuéllar, J., Gnesi, S., Latella, D.: FMICS special issue. Sci. Comput. Program. **36**(1), 1–3 (2000). https://doi.org/10.1016/S0167-6423(99)00014-3
31. Cunha, A., Macedo, N.: Validating the hybrid ERTMS/ETCS level 3 concept with Electrum. Int. J. Softw. Tools Technol. Transf. **22**(3), 281–296 (2020). https://doi.org/10.1007/s10009-019-00540-4
32. DaSilva, C., Dehbonei, B., Mejia, F.: Formal specification in the development of industrial applications: subway speed control system. In: Diaz, M., Groz, R. (eds.) FORTE 1992. IFIP, vol. C-10, pp. 199–213. North-Holland (1992)
33. Davis, J.A., et al.: Study on the barriers to the industrial adoption of formal methods. In: Pecheur, C., Dierkes, M. (eds.) FMICS 2013. LNCS, vol. 8187, pp. 63–77. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41010-9_5
34. Dghaym, D., Dalvandi, M., Poppleton, M., Snook, C.: Formalising the hybrid ERTMS level 3 specification in iUML-B and Event-B. Int. J. Softw. Tools Technol. Transf. **22**(3), 297–313 (2020). https://doi.org/10.1007/s10009-019-00548-w
35. Dollé, D., Essamé, D., Falampin, J.: B dans le transport ferroviaire: L'expérience de Siemens transportation systems. Tech. Sci. Inf. **22**(1), 11–32 (2003). https://doi.org/10.3166/tsi.22.11-32
36. Dongol, B., et al.: On formal methods thinking in computer science education. Form. Asp. Comput. (2024). https://doi.org/10.1145/36704
37. Essamé, D., Dollé, D.: B in large-scale projects: the Canarsie line CBTC experience. In: Julliand, J., Kouchnarenko, O. (eds.) B 2007. LNCS, vol. 4355, pp. 252–254. Springer, Heidelberg (2006). https://doi.org/10.1007/11955757_21
38. European Committee for Electrotechnical Standardization: CENELEC EN 50128: Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems (2011). https://standards.globalspec.com/std/1678027/cenelec-en-50128
39. Fantechi, A.: Twenty-five years of formal methods and railways: what next? In: Counsell, S., Núñez, M. (eds.) SEFM 2013. LNCS, vol. 8368, pp. 167–183. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-05032-4_13
40. Fantechi, A., Ferrari, A., Gnesi, S.: Formal methods and safety certification: challenges in the railways domain. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016. LNCS, vol. 9953, pp. 261–265. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47169-3_18
41. Fantechi, A., Flammini, F., Gnesi, S.: Formal methods for intelligent transportation systems. In: Margaria, T., Steffen, B. (eds.) ISoLA 2012. LNCS, vol. 7610, pp. 187–189. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34032-1_19
42. Fantechi, A., Flammini, F., Gnesi, S.: Formal methods for railway control systems. Int. J. Softw. Tools Technol. Transf. **16**(6), 643–646 (2014). https://doi.org/10.1007/s10009-014-0342-1

43. Fantechi, A., Gnesi, S., Haxthausen, A.E.: Formal methods for distributed computing in future railway systems. In: Margaria, T., Steffen, B. (eds.) ISoLA 2020. LNCS, vol. 12478, pp. 389–392. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-61467-6_24
44. Fantechi, A., Gnesi, S., Haxthausen, A.E.: Formal methods for distributed control systems of future railways. In: Margaria, T., Steffen, B. (eds.) ISoLA 2022. LNCS, vol. 13704, pp. 243–245. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-19762-8_19
45. Fantechi, A., Gnesi, S., Haxthausen, A.E.: Formal methods for DIStributed COmputing in future RAILway systems. In: Margaria, T., Steffen, B. (eds.) ISoLA 2024. Springer, LNCS (2024)
46. Ferrari, A., ter Beek, M.H.: Formal methods in railways: a systematic mapping study. ACM Comput. Surv. **55**(4), 69:1–69:37 (2023). https://doi.org/10.1145/3520480
47. Ferrari, A., et al.: Survey on formal methods and tools in railways: the ASTRail approach. In: Collart-Dutilleul, S., Lecomte, T., Romanovsky, A. (eds.) RSSRail 2019. LNCS, vol. 11495, pp. 226–241. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-18744-6_15
48. Ferrari, A., Fantechi, A., Magnani, G., Grasso, D., Tempestini, M.: The Metrô Rio case study. Sci. Comput. Program. **78**(7), 828–842 (2013). https://doi.org/10.1016/j.scico.2012.04.003
49. Ferrari, A., Mazzanti, F., Basile, D., ter Beek, M.H.: Systematic evaluation and usability analysis of formal methods tools for railway signaling system design. IEEE Trans. Softw. Eng. **48**(11), 4675–4691 (2022). https://doi.org/10.1109/TSE.2021.3124677
50. Flammini, F., Marrone, S., Nardone, R., Vittorini, V.: Compositional modeling of railway virtual coupling with stochastic activity networks. Form. Asp. Comput. **33**(6), 989–1007 (2021). https://doi.org/10.1007/S00165-021-00560-5
51. Garavel, H., ter Beek, M.H., van de Pol, J.: The 2020 expert survey on formal methods. In: ter Beek, M.H., Ničković, D. (eds.) FMICS 2020. LNCS, vol. 12327, pp. 3–69. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58298-2_1
52. Garavel, H., Gnesi, S., Schieferdecker, I.: Special issue on FMICS 2000. Sci. Comput. Program. **46**(3), 195–196 (2003). https://doi.org/10.1016/S0167-6423(02)00091-6
53. Ghazel, M.: A control scheme for automatic level crossings under the ERTMS/ETCS level 2/3 operation. IEEE Trans. Intell. Transp. Syst. **18**(10), 2667–2680 (2017). https://doi.org/10.1109/TITS.2017.2657695
54. Gnesi, S., Latella, D.: Special issue on FMICS 1996. Form. Methods Syst. Des. **12**(2), 123–124 (1998). https://doi.org/10.1023/A:1008669025349
55. Gnesi, S., Latella, D.: Special issue on FMICS 1997. Form. Asp. Comput. **10**(4), 311–312 (1998). https://doi.org/10.1007/s001650050019
56. Gnesi, S., Latella, D.: Special issue on FMICS 1999. Form. Methods Syst. Des. **19**(2), 119–120 (2001). https://doi.org/10.1023/A:1011279615774
57. Gnesi, S., Margaria, T.: Formal Methods for Industrial Critical Systems: A Survey of Applications. Wiley, Hoboken (2013). https://doi.org/10.1002/9781118459898
58. Groote, J.F., van Vlijmen, S.F.M., Koorn, J.W.C.: The safety guaranteeing system at station Hoorn-Kersenboogerd. In: COMPASS 1995, pp. 57–68 (1995). https://doi.org/10.1109/CMPASS.1995.521887
59. Guiho, G., Hennebert, C.: SACEM Software validation. In: ICSE 1990, pp. 186–191. IEEE (1990)

60. Hansen, D., et al.: Validation and real-life demonstration of ETCS hybrid level 3 principles using a formal B model. Int. J. Softw. Tools Technol. Transf. **22**(3), 315–332 (2020). https://doi.org/10.1007/s10009-020-00551-6
61. Haxthausen, A.E., Fantechi, A.: Compositional verification of railway interlocking systems. Form. Asp. Comput. **35**(1), 4:1–4:46 (2023). https://doi.org/10.1145/3549736
62. Himrane, O., Beugin, J., Ghazel, M.: Toward formal safety and performance evaluation of GNSS-based railway localisation function. IFAC-Pap. **54**(2), 159–166 (2021). https://doi.org/10.1016/j.ifacol.2021.06.049. Proceedings CTS 2021
63. Himrane, O., Beugin, J., Ghazel, M.: Implementation of a model-oriented approach for supporting safe integration of GNSS-based virtual balises in ERTMS/ETCS Level 3. IEEE Open J. Intell. Transp. Syst. **4**, 294–310 (2023). https://doi.org/10.1109/OJITS.2023.3267142
64. Hong, L.V., Haxthausen, A.E., Peleska, J.: Formal modelling and verification of interlocking systems featuring sequential release. Sci. Comput. Program. **133**, 91–115 (2017). https://doi.org/10.1016/j.scico.2016.05.010
65. James, P., Moller, F., Nga, N.H., Roggenbach, M., Schneider, S., Treharne, H.: Techniques for modelling and verifying railway interlockings. Int. J. Softw. Tools Technol. Transf. **16**(6), 685–711 (2014). https://doi.org/10.1007/S10009-014-0304-7
66. Kubczak, C., Margaria, T., Nagel, R., Steffen, B.: Plug and play with FMICS-jETI: beyond scripting and coding. ERCIM News **73**, 41–42 (2008). http://ercim-news.ercim.eu/plug-and-play-with-fmics-jeti-beyond-scripting-and-coding
67. Lecomte, T.: Safe and reliable metro platform screen doors control/command systems. In: Cuellar, J., Maibaum, T., Sere, K. (eds.) FM 2008. LNCS, vol. 5014, pp. 430–434. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68237-0_32
68. Limbrée, C., Pecheur, C.: A framework for the formal verification of networks of railway interlockings - application to the Belgian railway. Electron. Commun. EASST **76** (2018). https://doi.org/10.14279/TUJ.ECEASST.76.1077
69. Mammar, A., Frappier, M., Tueno Fotso, S.J., Laleau, R.: A formal refinement-based analysis of the hybrid ERTMS/ETCS level 3 standard. Int. J. Softw. Tools Technol. Transf. **22**(3), 333–347 (2020). https://doi.org/10.1007/s10009-019-00543-1
70. Marais, J., Beugin, J., Berbineau, M.: A survey of GNSS-based research and developments for the European railway signaling. IEEE Trans. Intell. Transp. Syst. **18**(10), 2602–2618 (2017). https://doi.org/10.1109/TITS.2017.2658179
71. Margaria, T., Kiniry, J.: Welcome to formal methods in industry. IT Prof. **22**(1), 9–12 (2020). https://doi.org/10.1109/MITP.2020.2968715
72. Margaria, T., Kubczak, C., Steffen, B., Naujokat, S.: The FMICS-jETI platform: status and perspectives. In: ISoLA 2006, pp. 402–407. IEEE (2006). https://doi.org/10.1109/ISOLA.2006.50
73. Margaria, T., Massink, M.: FMICS 2005. ACM (2005). https://doi.org/10.1145/1081180
74. Margaria, T., Massink, M.: Special section on FMICS 2005. Int. J. Softw. Tools Technol. Transf. **11**(5), 355–357 (2009). https://doi.org/10.1007/S10009-009-0121-6
75. Margaria, T., Raffelt, H., Steffen, B., Leucker, M.: The LearnLib in FMICS-jETI. In: ICECCS 2007, pp. 340–352. IEEE (2007). https://doi.org/10.1109/ICECCS.2007.43

76. Mazzanti, F., Ferrari, A., Spagnolo, G.O.: Experiments in formal modelling of a deadlock avoidance algorithm for a CBTC system. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016. LNCS, vol. 9953, pp. 297–314. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47169-3_22
77. Mazzanti, F., Spagnolo, G.O., Della Longa, S., Ferrari, A.: Deadlock avoidance in train scheduling: a model checking approach. In: Lang, F., Flammini, F. (eds.) FMICS 2014. LNCS, vol. 8718, pp. 109–123. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10702-8_8
78. Meo, C.D., Di Vaio, M., Flammini, F., Nardone, R., Santini, S., Vittorini, V.: ERTMS/ETCS virtual coupling: proof of concept and numerical analysis. IEEE Trans. Intell. Transp. Syst. **21**(6), 2545–2556 (2020). https://doi.org/10.1109/TITS.2019.2920290
79. Ramnath, S., Walk, S.: Structuring formal methods into the undergraduate computer science curriculum. In: Benz, N., Gopinath, D., Shi, N. (eds.) NFM 2024. LNCS, vol. 14627, pp. 399–405. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-60698-4_24
80. Seisenberger, M., et al.: Safe and secure future AI-driven railway technologies: challenges for formal methods in railway. In: Margaria, T., Steffen, B. (eds.) ISoLA 2022. LNCS, vol. 13704, pp. 246–268. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-19762-8_20
81. Tueno Fotso, S.J., Frappier, M., Laleau, R., Mammar, A.: Modeling the hybrid ERTMS/ETCS level 3 standard using a formal requirements engineering approach. Int. J. Softw. Tools Technol. Transf. **22**(3), 349–363 (2020). https://doi.org/10.1007/s10009-019-00542-2
82. The White House: Back to the Building Blocks: A Path Toward Secure and Measurable Software. Tech. rep., White House Office of the National Cyber Director (ONCD) (2024). https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf
83. X2Rail-2 – Deliverable D5.1, Formal Methods (Taxonomy and Survey), Proposed Methods and Applications (2018). https://projects.shift2rail.org/download.aspx?id=b4cf6a3d-f1f2-4dd3-ae01-2bada34596b8