Formal Methods and Tools Applied in the Railway Domain

Maurice H. ter Beek(✉)

Formal Methods and Tools Lab, CNR–ISTI, Pisa, Italy
maurice.terbeek@isti.cnr.it

Abstract. ABZ and other state-based formal methods and tools are successfully applied to the development of safety-critical systems for decades now, in particular in the transport domain, without a single language or tool emerging as the dominant solution for system design. Formal methods are highly recommended by the current safety standards in the railway industry, but railway engineers often lack the knowledge to transform their semi-formal models into formal models, with a precise semantics, to serve as input to formal methods tools. We share the results of performing empirical studies in the railway domain, including usability analyses of formal methods tools involving railway practitioners. We discuss, in particular with respect to railway systems and their modelling, our experiences in applying rigorous state-based methods and tools to a variety of case studies, for which we interacted with a number of companies from the railway domain. We report on lessons learned from these experiences and provide pointers to drive future research towards facilitating further synergies between—on the one hand—researchers and developers of ABZ and other state-based formal methods and tools, and—on the other hand—practitioners from the railway industry.

1 Introduction

For decades now, railways are controlled by real-time computer-based systems. To fulfil stringent safety requirements, railway control systems typically require extensive verification and validation, largely relying on formal methods, as highly recommended by the CENELEC European standards [30,51] for the development of the most critical software for use in the railway industry. This is also witnessed by hundreds of recent projects financed as part of the European Shift2Rail Joint Undertaking[1] and its successor Europe's Rail[2] and as part of related initiatives outside the EU, like the UK Rail Research and Innovation Network (UKRRIN)[3] and the Chinese State Key Laboratory of Rail Traffic Control and Safety[4].

The original version of the chapter has been revised. A correction to this chapter can be found at https://doi.org/10.1007/978-3-031-63790-2_31

[1] https://shift2rail.org/.
[2] https://rail-research.europa.eu/.
[3] https://www.ukrrin.org.uk/.
[4] http://en.bjtu.edu.cn/research/institute/laboratory/16583.htm.

S. Bonfanti et al. (Eds.): ABZ 2024, LNCS 14759, pp. 3–21, 2024.
https://doi.org/10.1007/978-3-031-63790-2_1

We participated in the Shift2Rail projects ASTRail[5] and 4SECURail[6] and in the Italian regional projects TRACE-IT (TRAin Control Enhancement via Information Technology), STINGRAY (SmarT station INtelliGent RAilwaY) and SmaRIERS (Smart Railway Infrastructures: Efficiency, Reliability and Safety). Through these projects we interacted with a number of companies from the railway domain, which allowed us to apply more than three decades of experience with formal methods and tools accumulated in our research lab FMT (Formal Methods and Tools) to a variety of case studies from the railway domain.

The main safety-critical railway signalling systems can be classified in two large classes of applications: train movement and distancing control systems, including the Automatic Train Control (ATC), Automatic Train Operation (ATO), Automatic Train Protection (ATP) and Automatic Train Supervision (ATS) subsystems, and interlocking systems. All these 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 aforementioned 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 rigorous state-based B method to many cases, which include the verification of the ATP system for the RER Line A of Paris [61], the Subway Speed Control System (SSCS) of the Calcutta subway [44], and Line 14 of the Paris Metro [48], as well as derivatives thereof, like line 1 or the NY Canarsie line [50], and the driverless Paris–Roissy Airport shuttle [25]. Moreover, B was also used for an industrial scale analysis of Alstom's U400 system [41], which is in operation in about 100 metro lines worldwide.

Further success stories of applying formal methods and tools to railway systems include the metro control system of Rio de Janeiro, with the support of Simulink/Stateflow [54], the ERTMS/ETCS standard with NuSMV [36] and Hybrid ERTMS/ETCS Level 3 with several formal methods and tools as part of the ABZ 2018 case study [4,7,34,42,47,63,77,88]. Moreover, in [6], the system structure of a movement authority scenario of CTCS Level 3 was modelled in AADL [84] and Hybrid CSP [68], and verified with the Hybrid Hoare Logic Prover [89], an interactive theorem prover based on Isabelle/HOL [92]. Recently, in [21], the autonomous positioning system in development for the Florence tramways was verified with the UPPAAL model-checking toolset [26,46].

In this paper, we first share the results of performing empirical studies in the railway domain, including usability analyses of formal methods tools involving railway practitioners, in Sects. 2 and 3. We then present some applications of formal methods and tools to case studies from the railway domain in Sect. 4, reporting some lessons learned from these experiences and providing some pointers to drive future research in the concluding Sect. 5.

[5] http://www.astrail.eu/.
[6] https://www.4securail.eu/.

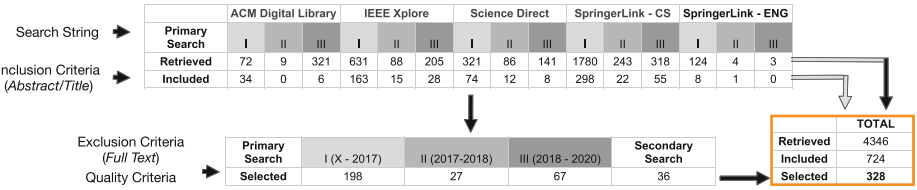

Fig. 1. Process of study selection and numerical results. The value of TOTAL in the bottom-right table is obtained by summing-up the cells in Retrieved, Included and Selected from the other tables. ©2022 ACM. Reprinted (and annotated) with permission from ACM Computing Surveys [52].

2 Systematic Mapping Study

In [52], we presented the first systematic mapping study[7] on formal methods in the railway domain, focusing on railway signalling systems, to complement other empirical studies that we performed, which considered the perspective of stakeholders [15,22] and surveyed different tools for railway system design [55,56,79] (cf. Sect. 3). Starting from the base terms "formal methods" (representing the object of research) and "railways" (representing the domain of application), we used alternative keywords and wildcards to elaborate the following search string:

"formal" OR "model check*" OR "model based" OR "model driven" OR "theorem prov*" OR "static analysis"

AND

"railway*" OR "CBTC" OR "ERTMS" OR "ETCS" OR "interlocking" OR "automatic train" OR "train control" OR "metro" OR "CENELEC"

As shown in Fig. 1, after originally retrieving 4346 studies from four main scientific databases, eventually 328 high-quality studies were selected from the literature from the period 1989–2020. These 328 papers were analysed in detail.

Figure 2 shows that formal methods for railways is a hot topic with a strong industrial focus, given that 143 papers were published solely during the last five years (44% of the total), while no less than 79 papers (24%) involve industry (papers with at least one industrial co-author).

Figure 3 shows that models are at the basis of practically all papers and that formal verification and model checking are the main analysis techniques [9,39], but also simulation [64], theorem proving [80,83] and refinement [2,3,74] are prominently applied techniques.

In terms of concrete languages and tools, Figs. 4 and 5 illustrate that the landscape is highly diversified, but B (15% in total and 22% of the industrial papers) [1,8,25,41,59,63,67,76,87] and ProB (9% in both cases) [1,41,63,67,76,87] are among the dominant languages and frequently used tools. However, there are examples also of ASM, VDM, Z, Alloy and TLA+ [35,57,70], as well as of Atelier-B and Rodin [4,40,41,65,82,88]. Tools of the B family (i.e., ProB, Atelier-B and Rodin) clearly dominate (18% overall and 20% of the industrial papers).

[7] A variant of systematic literature reviews aiming at classifying the literature [71,81].

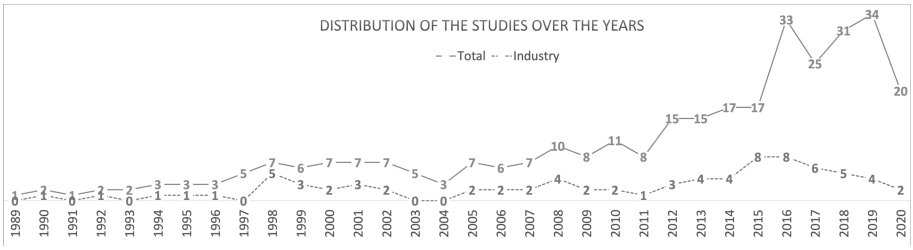

Fig. 2. Studies by year. ©2022 ACM. Reprinted with permission from ACM Computing Surveys [52].

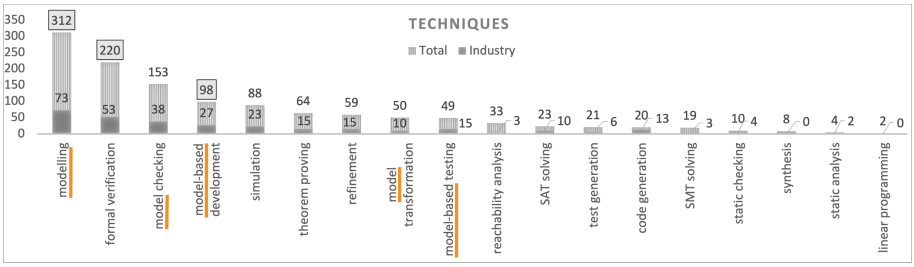

Fig. 3. Techniques. ©2022 ACM. Reprinted (and annotated) with permission from ACM Computing Surveys [52].

Our systematic mapping study shows that the empirical maturity of the field is still limited, as many of the selected papers present only examples or experience reports. We call for more empirical rigor in the field, with case studies, which can leverage the strong link with industries, and for controlled experiments, which can address issues related to the learnability of formal methods and aspects related to human factors. In fact, many papers do not focus on a particular railway system or standard, but we signal an improvement with high-quality papers on the ERTMS/ETCS [28,63], CBTC [41] and CTCS [11] standards. Interlocking is still the most popular subject of study, but other railway subsystems (e.g., ATC, ATO, ATP and ATS) are being considered more frequently in recent years [62,90,91]. ABZ has contributed to this goal with the Hybrid ERTMS/ETCS Level 3 case study at ABZ 2018 [4,7,34,42,47,63,77,88].

Our findings also show that almost all core railway development phases can be addressed with the support of formal methods, which is in line with the recommendations of the norms [30,51]. However, additional effort should be dedicated to the later phases of the development process, in particular testing, implementation and validation, which are currently apparently not sufficiently addressed.

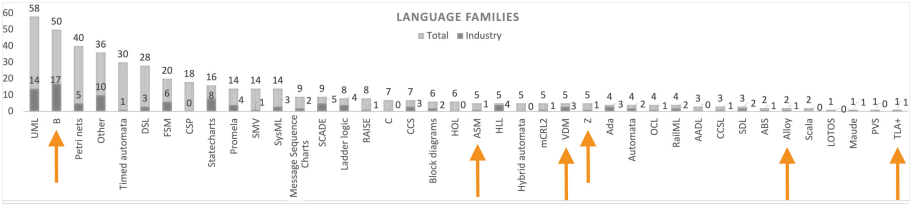

Fig. 4. Modeling language families considered in the studies. ©2022 ACM. Reprinted (and annotated) with permission from ACM Computing Surveys [52].

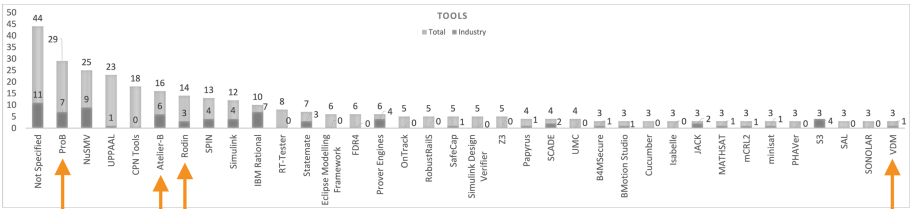

Fig. 5. Tools. ©2022 ACM. Reprinted (and annotated) with permission from ACM Computing Surveys [52].

3 Systematic Evaluation and Usability Analysis

In [55], we presented the first systematic tool evaluation[8] and usability analysis of formal methods tools for railway signalling system design. This complements other empirical studies that we performed, which surveyed various tools for railway system design [56,79] selected based on surveys with stakeholders [22,53] and a literature review [52] (cf. Sect. 2). The 13 selected tools are as follows: SPIN, Simulink, nuXmv, ProB, Atelier-B, UPPAAL, FDR4, CPN Tools, CADP, mCLR2, SAL, TLA+ and UMC (cf. [55] for individual references to these tools[9]).

The research questions (RQs) we posed ourselves in [55] were the following:

RQ1: *Which are the features to consider for evaluating a formal methods tool?*
RQ2: *How do different tools compare with respect to these features?*
RQ3: *How do different tools compare with respect to their usability?*

Table 1 summarises the characteristics and expertise of the participants who evaluated the tools based on direct hands-on experience. Next to the assessors and academic experts (including the authors of [55]), we involved nine railway practitioners as industry experts, who had no prior experience with applying formal methods tools yet more than 10 years of experience in the railway domain.

[8] Based on the DESMET methodology for evaluating software engineering tools [72].
[9] In [55], UPPAAL denoted all variants (i.e., UPPAAL 4.0, UPPAAL SMC, UPPAAL Stratego and UPPAAL Tiga), by now integrated in UPPAAL 5: https://uppaal.org/.

Table 1. Characteristics and expertise of the study participants. Reprinted (and adapted) with permission from IEEE Transactions on Software Engineering [55].

ID	Role in Study	Milieu	Main Function	Age	Sex	Years of Experience in		
						Formal Methods (FM)	Railway Industry	FM in Railways
1	assessor	academic	workpackage leader	39	M	>13	3	13
2	assessor	academic	tool developer	62	M	>20	0	9
3	assessor	academic	researcher	36	M	>6	0	4
4	expert	academic	group leader	48	M	>15	0	9
5	expert	academic	project leader	66	F	>30	0	>25
6	expert	academic	professor	65	M	>30	0	>25
7	expert	industry	system engineer	NA	M	0	>10	0
8	expert	industry	system engineer	52	M	0	>10	0
9	expert	industry	system engineer	48	M	0	>10	0
10	expert	industry	software developer	43	M	0	>10	0
11	expert	industry	product manager	NA	M	0	>10	0
12	expert	industry	system engineer	48	M	0	>10	0
13	expert	industry	innovation engineer	NA	M	0	>10	0
14	expert	industry	software developer	45	M	0	>10	0
15	expert	industry	innovation engineer	NA	F	0	3 to 10	0

The systematic feature evaluation was performed by the assessors, after elicitating the features with a collaborative approach inspired by the KJ method [85]. During a 3 h workshop, the assessors, the academic experts and two industry experts came up with 33 features that should be considered when evaluating a formal methods tool for railway system design, hierarchically categorized into functional, expressiveness, and quality features, comprising 8 subcategories. The assessors produced an evaluation sheet for each tool based on the following use:

1. install and run the tool;
2. consult the tool's website for official documentation;
3. search for additional documentation useful to fill the evaluation sheet;
4. consult the 114 papers on formal methods and railways from the literature review [53] to check for the tool's application in railways;
5. perform some trials with the tool to confirm the claims reported in the documentation, and assign the value to those features that required hands-on activity to be evaluated;
6. report the evaluation on the sheet, together with links to the consulted documents and papers, and appropriate notes when the motivation of an assignment needed clarification.

The evaluation sheets were revised after face-to-face meetings to align visions and balance judgments, and reviewed externally as part of a deliverable of the ASTRail project, and they are publicly available for inspection [79]. Figure 6 reports the table resulting from the feature evaluation activity.

Category	Name	SPIN	Simulink	nuXmv	ProB	Atelier B	UPPAAL	FDR4	CPN Tools	CADP	mCRL2	SAL	TLA+	UMC
Development Functionalities	Specification / Modeling	TEXT	GRAPH	TEXTIM	TEXT	TEXT	GRAPH	TEXTIM	GRAPH	TEXTIM	TEXT	TEXTIM	TEXT	TEXT
	Code Generation	NO	YES	NO	NO	YES	NO	NO	NO	YES	NO	NO	NO	NO
	Documentation / Report Generation	PARTIAL	YES	NO	PARTIAL	PARTIAL	PARTIAL	PARTIAL	NO	PARTIAL	PARTIAL	NO	NO	PARTIAL
	Requirements Traceability	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Project Management	NO	YES	NO	YES	YES	NO	NO	NO	NO	NO	NO	NO	NO
Verification Functionalities	Simulation	TEXT	GRAPH	TEXT	MIX	NO	GRAPH	TEXT	GRAPH	TEXT	TEXT	TEXT	NO	TEXT
	Formal Verification	MC-L	MC-O	MC-L,MC-B	MC-L,MC-B,RF	TP	MC-L,RF	RF	MC-B	MC-B,RF	MC-B,RF	MC-L,TP	MC-L,TP	MC-B
	Large-scale Verification Technique	FLY,POR,PAR	BMC	BMC,SYM	SCT	SCT	SMC,SYM	COM,POR	BMC	COM,PAR	COM	PAR,SCT	SYM,SCT	FLY
	Model-based Testing	NO	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	NO
Language Expressiveness	Non-determinism	INT	EXT	INT,EXT	INT,EXT	INT,EXT	INT,EXT	INT,EXT	INT	INT,EXT	INT,EXT	INT,EXT	INT	INT
	Concurrency	ASYNCH	NO	SYNCH	NO	NO	SYNCH	ASYNCH	ASYNCH	ASYNCH	ASYNCH	A/SYNCH	ASYNCH	A/SYNCH
	Timing Aspects	NO	YES	YES	NO	NO	YES	YES	YES	NO	YES	YES	NO	NO
	Stochastic or Probabilistic Aspects	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	NO	NO	NO
	Modularity of the Language	HIGH	HIGH	MEDIUM	LOW	LOW	MEDIUM	HIGH	HIGH	HIGH	HIGH	MEDIUM	MEDIUM	HIGH
	Supported Data Structures	BASIC	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX
	Float Support	NO	YES	YES	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO
Tool Flexibility	Backward Compatibility	LIKELY	LIKELY	LIKELY	LIKELY	MODERATE	LIKELY	MODERATE	LIKELY	LIKELY	LIKELY	MODERATE	MODERATE	MODERATE
	Standard Input Format	OPEN	PARTIAL	OPEN	OPEN	OPEN	PARTIAL	OPEN	PARTIAL	STANDARD	OPEN	OPEN	OPEN	STANDARD
	Import / Export vs. Other Tools	MEDIUM	LOW	MEDIUM	HIGH	MEDIUM	LOW	MEDIUM	MEDIUM	HIGH	HIGH	MEDIUM	LOW	MEDIUM
	Modularity of the Tool	LOW	HIGH	LOW	HIGH	MEDIUM	HIGH	LOW	LOW	HIGH	MEDIUM	LOW	LOW	MEDIUM
	Team Support	NO	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO
Maturity	Industrial Diffusion	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	MEDIUM	MEDIUM	MEDIUM	MEDIUM	LOW	MEDIUM	LOW
	Stage of Development	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	PROTOTYPE
Usability	Availability of Customer Support	PARTIAL	YES	PARTIAL	YES	YES	YES	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL
	Graphical User Interface	LIMITED	YES	NO	PARTIAL	PARTIAL	YES	LIMITED	PARTIAL	LIMITED	PARTIAL	NO	LIMITED	PARTIAL
	Mathematical Background	MEDIUM	BASIC	MEDIUM	MEDIUM	ADVANCED	MEDIUM	ADVANCED	MEDIUM	ADVANCED	ADVANCED	ADVANCED	ADVANCED	MEDIUM
	Quality of Documentation	GOOD	EXCELLENT	GOOD	GOOD	EXCELLENT	GOOD	EXCELLENT	GOOD	GOOD	GOOD	GOOD	GOOD	LIMITED
Company Constraints	Cost	FREE	PAY	MIX	FREE	FREE	MIX	MIX	FREE	MIX	FREE	FREE	FREE	FREE
	Supported Platforms	ALL	ALL	ALL	ALL	ALL	ALL	ALL	Windows	ALL	ALL	ALL	ALL	ALL
	Complexity of License Management	EASY	ADEQUATE	EASY	EASY	EASY	MODERATE	MODERATE	EASY	MODERATE	EASY	EASY	EASY	EASY
	Easy to Install	YES	YES	YES	YES	YES	YES	YES	YES	PARTIAL	YES	YES	YES	YES
Railway-specific Criteria	CENELEC Certification	NO	PARTIAL	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Integration in the CENELEC Process	MEDIUM	YES	MEDIUM	YES	YES	MEDIUM	MEDIUM	MEDIUM	MEDIUM	LOW	LOW	LOW	MEDIUM
		SPIN	Simulink	nuXmv	ProB	Atelier B	UPPAAL	FDR4	CPN Tools	CADP	mCRL2	SAL	TLA+	UMC

Fig. 6. Evaluation table. ©2021 IEEE. Personal use is permitted, but republication/ redistribution requires IEEE permission. Reprinted (and annotated) with permission from IEEE Transactions on Software Engineering [55].

We note that ProB and Atelier-B stand out for project management and score well on tool flexibility (Atelier-B is the only tool including team support), usability and maturity; TLA+ much less.

We selected a subset of seven tools for the usability evaluation, excluding those requiring advanced mathematical background (except for Atelier-B, since it is one of the few tools used in the development of real-world railway products, cf. "Integration in the CENELEC process" in Fig. 6) and those for which it is known from the literature that they are inadequate for handling industry-size problems. We performed the usability evaluation of the resulting seven tools (SPIN, Simulink, nuXmv, ProB, Atelier-B, UPPAAL and UMC) with railway experts adopting the following methodology.

First, the assessors developed a model of the moving block system for each of the tools. The experts were already familiar with the sample system, which has moreover been used as a reference by other papers in the literature [34,56].

Next, the different characteristics of the tools were illustrated in a 3 h meeting with the experts, using the predeveloped models as reference. The experts were asked to evaluate the usability of each tool based on their first impression. After an introduction, each tool was presented in a 15 min demo, covering the tool's general structure, then opening, navigating and describing the model, followed by a guided simulation and a description and presentation of a formal verification session. After the presentation of each tool, the experts filled a usability questionnaire for the tool.

We used the widely adopted System Usability Scale (SUS) questionnaire of Brooke [31,32], following Brooke's guidelines [31] to calculate the SUS score and

Bangor et al. [10] for the interpretations for the scores: 100 = Best Imaginable; 85 = Excellent; 73 = Good; 52 = OK; 39 = Poor; 25 = Worst Imaginable.

Figure 7 presents the results of the SUS questionnaire. The tool that clearly stands out as being considered the most usable is Simulink (SUS Score = 76.39), with ProB (62.22) as runner-up, whereas Atelier-B (45.56) is considered among the least usable tools, which is attributed to the refinement-based theorem-proving approach that requires mastering advanced skills. Overall, tool usability is acceptable, given the average SUS Score (56.67) between OK and Good.

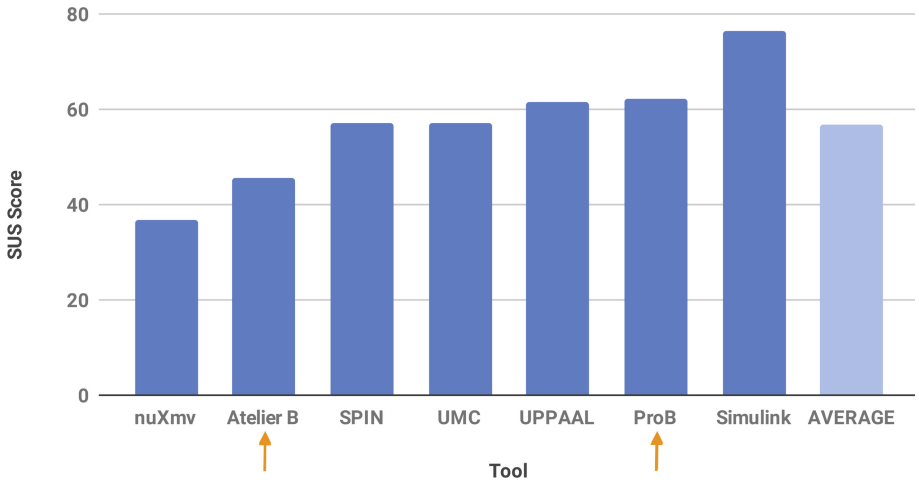

Fig. 7. SUS scores for the different tools. ©2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. Reprinted (and annotated) with permission from IEEE Transactions on Software Engineering [55].

4 Success Stories

In this section, we briefly discuss some of our experiences in applying rigorous state-based formal methods and tools to case studies that resulted from our participation in European Shift2Rail projects like ASTRail and 4SECURail and Italian regional projects like TRACE-IT, STINGRAY and SmaRIERS with industrial partners from the railway domain.

4.1 Next Generation Railway Signalling Systems

The railway domain is known to be cautious concerning the adoption of technological innovations, in particular when compared with other transport domains. Hence, while satellite-based positioning systems are in use for quite some time now in the avionics and automotive domains, current railway signalling systems

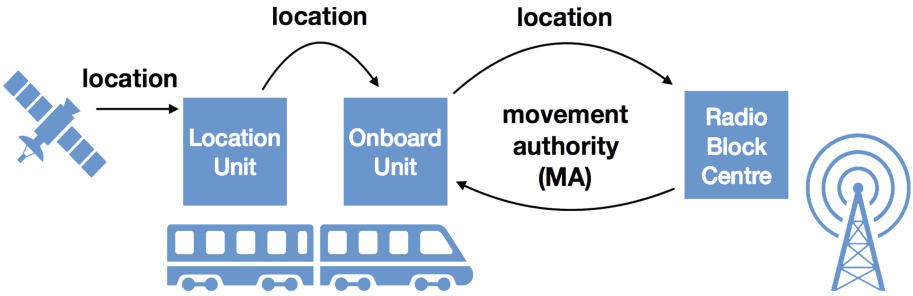

Fig. 8. ERTMS/ETCS Level 3 moving block railway signalling (reprinted from [17]).

still typically use traditional ground-based train detection systems with fixed block distancing. So-called ERTMS/ETCS Level 2 signalling systems make use of trackside equipment like track circuits or axle counters for exact train position detection and train integrity supervision and of fixed blocks starting and ending at signals, with the block sizes being determined by parameters like the speed limit, the train's speed and braking characteristics and the drivers' sighting and reaction times. Yet, the faster trains are allowed to run, the longer their worst-case braking distance, resulting in an increased safety distance and a decreased line capacity. Therefore, to increase the competitiveness, robustness and attractiveness of the railway domain, a recognised challenge consists of transitioning to the next generation of railway signalling system based on effective, precise moving block signalling systems by GNSS-based satellite positioning [58,78].

Such next generation ERTMS/ETCS Level 3 signalling systems no longer rely on trackside equipment for train position detection and train integrity supervision, but an onboard odometry system is responsible for monitoring the train's position and autonomously computing its current speed. This onboard unit frequently sends the train's position to a radio block centre which, in turn, sends each train a movement authority, computed by exploiting its knowledge of the position of the rear end of the train ahead (cf. Fig. 8). The resulting moving block signalling systems allow trains in succession to close up, since a safe zone around the moving trains can be computed, thus considerably reducing headways between trains, in principle to the braking distance (cf. Fig. 9). This allows for more trains to run on existing railway tracks and the removal of trackside equipment moreover results in lower capital and maintenance costs [58].

Starting with our involvement in ASTRail, we contributed to the many experiments and case studies being conducted and validated before actually moving to ERTMS/ETCS Level 3 signalling systems [4,7,12,13,16,28,29,34,42,47,63,77,88]. In [13,16], we presented Simulink [43] models for a simplified moving block specification with only one train, and used UPPAAL SMC [46] for formal verification and sensitivity analysis based on Statistical Model Checking (SMC) [5,75].

In [17], we presented an extension and refinement of the aforementioned UPPAAL model, consider more trains which concurrently communicate with the

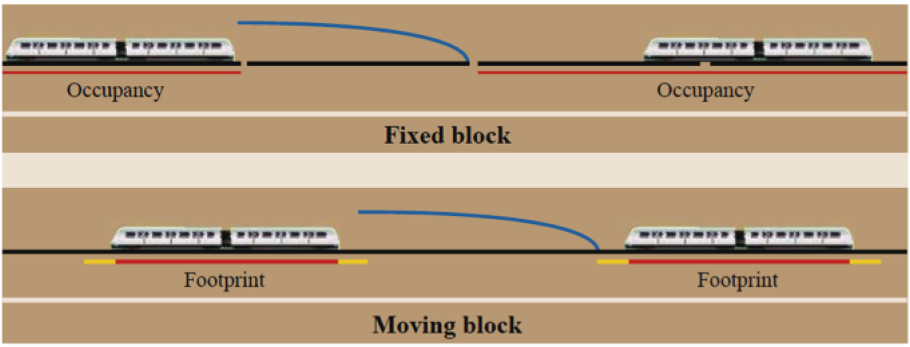

Fig. 9. Safe braking distance between trains for fixed block and moving block signalling (Image courtesy of Israel.abad/Wikimedia Commons distributed under the CC BY-SA 3.0 license).

same (trackside) radio block centre. The movement authority that was previously considered constant, was now computed dynamically according to the traffic on the railway line, and in particular the tail of the train ahead. The physical behaviour of the trains was tuned and validated according to parameters about high-speed trains from the literature [69]. We formally verified the correctness of the function that computes the movement authority, formalised in first-order logic. The concurrent nature of the radio block centre led to the detection and mitigation of corner cases. We also carried out experiments to validate candidate parameter setups to reduce the risk of trains exceeding their movement authority.

4.2 Synthesis of Autonomous Driving Strategies

In [18], we performed the first application of synthesis techniques to autonomous driving for next generation railway signalling systems. As described in the previous section, the Simulink and UPPAAL SMC models from [13,16] offered the possibility to fine tune communication parameters that are fundamental for the reliability of their operational behaviour; however, they did not account for the synthesis of autonomous driving strategies. In [18], we presented a UPPAAL Stratego [45] model (i.e., a stochastic priced timed game) of a satellite-based moving block railway signalling system that does account for autonomous driving. The autonomous driving module was not modelled manually, but it was synthesised automatically as a strategy based on a safety requirement that the model must respect, after which both standard and statistical model checking were applied under the resulting (safe) strategy. We moreover considered reliability aspects, and the autonomous driving strategy also provided guarantees for the minimal expected arrival time. It must be noted that the original model had to be simplified considerably to undergo strategy synthesis and verification, since UPPAAL SMC scales well to large systems by applying simulations rather than full state-space explorations whereas UPPAAL Stratego requires full state-space exploration of the timed game for strategy synthesis.

This was our first experience with strategy synthesis and optimisation of a case study from the railway domain and also with UPPAAL Stratego. This is a very recent formal methods tool which has not been much experimented with. In fact, while developing the model we ran into corner cases that needed interactions with the developers, which led to the release of new versions, with patches fixing the issues discovered through our modelling efforts.

A promising line of future research would be to adapt the statistical synthesis techniques described in [66] to learn safety objectives, thus avoiding the full state-space exploration (as currently performed in UPPAAL Stratego) while guaranteeing the scalability of SMC. This would enable the modelling of more complex case studies from the railway domain.

4.3 Smart Railway Systems and Stations of the Future

Traditionally, railway stations have a private energy distribution and communication system, mainly to ensure uninterrupted power supply and security. However, there are important drawbacks, such as prohibiting proper integration in the smart cities concept by exploiting information between different transport systems (e.g., bike sharing, car sharing, urban transport) and failing to benefit from state-of-the-art energy-saving techniques. In STINGRAY and SmaRIERS, we aimed to enhance the integration of railway stations into smart cities of the future and study advanced energy-saving techniques. In this section, we report work on two project case studies on smart energy consumption.

In [14], we performed a comparison of formal methods tools by experimenting the modelling and analysis features of Möbius [38] and UPPAAL SMC. As in Sect. 3, we applied both tools to the same case study. This time, the features on which we compared them ranged from modelling (e.g., communication primitives and delay distributions) to property specification (e.g., measures of interest) and experiments and presentation of results (e.g., experiment parameter setup). The case study concerns a cyber-physical system from the railway domain, namely a railroad switch heater that is meant to assure the correct operation of switches in case of ice and snow through a central control unit in charge of managing policies of energy consumption while satisfying reliability constraints. It contains physical components (the heater), cyber components (the heating policies and the related coordinator), stochastic aspects (failure events and weather forecasts), and logical/physical dependencies. The models and analyses with stochastic activity networks and Möbius were originally presented in [19], whereas those with stochastic hybrid automata and UPPAAL SMC were originally presented in [20].

To improve their usability, we concluded that Möbius could provide primitive support for non-anonymous replicas and channel communication (a suggestion which has since been implemented by the tool's developers), graphical visualisation of data and primitive support for ordinary differential equations, whereas UPPAAL SMC could provide primitive support for batches of experiments with different parameters (a suggestion which was well received by one of the tool's main developers) and further distribution delays (e.g., deterministic time).

In [24], we addressed the design of future smart station lighting management applications, which aim to reduce station illumination whenever (time) and wherever (space) possible while guaranteeing minimum illumination levels as required by current legislation. The (ceiling) lights (LEDs) along a station's platforms are equipped with a data acquisition module called MADILL. A C-MAD unit collects the messages from each MADILL and it is equipped with brightness sensors and commands to switch lights on, off, or dim them—either individually or for groups of lights.

We considered user-experience related requirements like "passengers should always be able to rely on an illuminated pathway when getting off or on a train, from the main entrance, to the platform", to avoid passengers transiting or waiting in non-illuminated areas, with the associated risks (e.g., theft or injury), or "there should be an illumination level greater than x on platforms where a train is about to arrive, even if the train is late". Such requirements are inherently spatial or spatio-temporal, as they deal with the possibly complex reachability relations and pathways of a train station. We envisioned how to tackle these concretely by applying spatial model-checking techniques and the VoxLogicA tool [27,37], as illustrated in Fig. 10 through images produced by VoxLogicA.

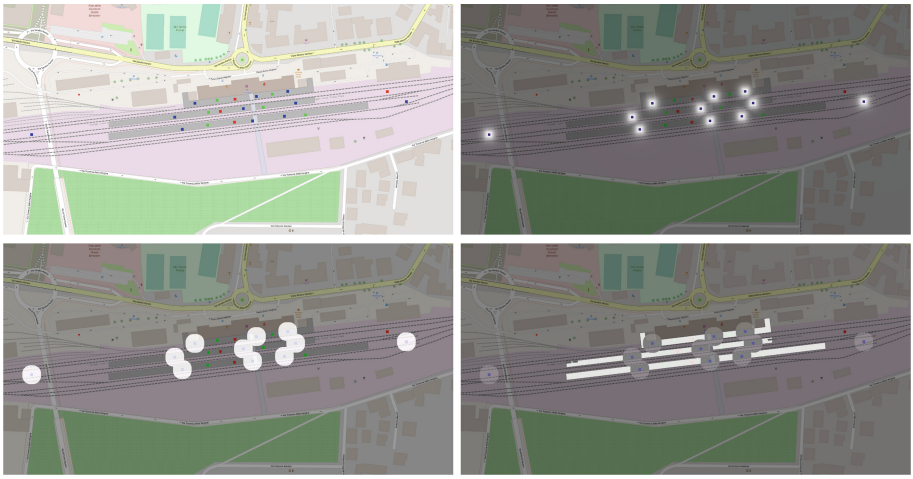

Fig. 10. Illustration of an experiment aimed at identifying poorly illuminated platform areas. **Top-left:** Pistoia station. Blue squares: a design with MADILL units, clearly insufficient in number. Red squares: some C-MAD units. Green squares: indicate the platforms open to the public. **Top-right:** illumination computed using an attenuation formula with VoxLogicA (overlay is made with an external program). **Bottom-left:** by a threshold on the illumination value, areas that are sufficiently illuminated have been computed (output from VoxLogicA). **Bottom-right:** the parts of the platforms that are not sufficiently illuminated are computed using VoxLogicA (shown in white). (Color figure online, reprinted from [24]).

5 Conclusion

Railway transportation by train, metro or tram is among the most environmentally friendly and energy-efficient means of transportation. In the near future, the railway domain is expected to contribute significantly to the European Green Deal by improved digitalisation and data analytics[10]. Current challenges include the extension of formal methods and tools to cope with AI-based systems, such as equipping verification tools with certificate generation, and their integration into the CENELEC standards [86]. There are, however, several limiting factors.

First, we need to close the gap between semi-formal models that are popular and suitable to communicate with industry and the formal models that are required to apply formal methods tools in safety-critical domains, like railways. Furthermore, each formal methods tool currently requires modelling expertise in a different input language and expert knowledge of different analysis techniques, making it important to pick the right tool based on input from industry and the requirements at hand. While it is no problem, or even a plus, for our FMT lab to host researchers with many different and complementary expertises, in-house expertise on formal methods tools is rare in industry (AWS and ASML are notable exceptions [23]).

Hence, the road to success that we foresee is to start from the basis, i.e., we, together with many experts [60], advocate a prominent role of formal methods in computer science education. First, there is the importance of formal methods *thinking* in computer science education [49], which provides the necessary rigour in reasoning on correctness, and the fundamental skill of abstraction [73]. Then, there is the importance of *knowing* formal methods [33], since the skills and knowledge acquired from studying formal methods provide the indispensable solid foundation that forms the backbone of computer science practice. This is confirmed by the recent increase in *using* formal methods in industry [23,60], not limited to the safety-critical domain.

Acknowledgements. Thanks to all co-authors of the work recollected in this invited contribution: Davide Basile, Vincenzo Ciancia, Felicita Di Giandomenico, Alessandro Fantechi, Alessio Ferrari, Stefania Gnesi, Diego Latella, Axel Legay, Mieke Massink, Franco Mazzanti, and Giorgio Spagnolo.

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

References

1. Abo, R., Voisin, L.: Formal implementation of data validation for railway safety-related systems with OVADO. In: Counsell, S., Núñez, M. (eds.) SEFM 2013. LNCS, vol. 8368, pp. 221–236. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-05032-4_17

[10] https://transport.ec.europa.eu/system/files/2021-04/2021-mobility-strategy-and-action-plan.pdf.

2. Abrial, J.: Refinement, decomposition and instantiation of discrete models. In: Proceedings of the 12th International Workshop on Abstract State Machines (ASM 2005), pp. 17–40 (2005)
3. Abrial, J.: Modeling in Event-B: System and Software Engineering. Cambridge University Press, Cambridge (2010). https://doi.org/10.1017/CBO9781139195881
4. 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
5. Agha, G., Palmskog, K.: A survey of statistical model checking. ACM Trans. Model. Comput. Simul. **28**(1), 6:1–6:39 (2018). https://doi.org/10.1145/3158668
6. 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
7. 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
8. Badeau, F., Amelot, A.: Using B as a high level programming language in an industrial project: Roissy VAL. In: Treharne, H., King, S., Henson, M., Schneider, S. (eds.) ZB 2005. LNCS, vol. 3455, pp. 334–354. Springer, Heidelberg (2005). https://doi.org/10.1007/11415787_20
9. Baier, C., Katoen, J.P.: Principles of Model Checking. MIT Press, Cambridge (2008)
10. Bangor, A., Kortum, P.T., Miller, J.T.: An empirical evaluation of the system usability scale. Int. J. Hum. Comput. Interact. **24**(6), 574–594 (2008). https://doi.org/10.1080/10447310802205776
11. Bao, Y., Chen, M., Zhu, Q., Wei, T., Mallet, F., Zhou, T.: Quantitative performance evaluation of uncertainty-aware hybrid AADL designs using statistical model checking. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **36**(12), 1989–2002 (2017). https://doi.org/10.1109/TCAD.2017.2681076
12. 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
13. Basile, D., ter Beek, M.H., Ciancia, V.: Statistical model checking of a moving block railway signalling scenario with Uppaal SMC. In: Margaria, T., Steffen, B. (eds.) ISoLA 2018. LNCS, vol. 11245, pp. 372–391. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03421-4_24
14. Basile, D., ter Beek, M.H., Di Giandomenico, F., Fantechi, A., Gnesi, S., Spagnolo, G.O.: 30 years of simulation-based quantitative analysis tools: a comparison experiment between Möbius and Uppaal SMC. In: Margaria, T., Steffen, B. (eds.) Leveraging Applications of Formal Methods, Verification and Validation: Verification Principles. ISoLA 2020. LNCS, vol. 12476, pp. 368–384. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-61362-4_21
15. 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
16. Basile, D., ter Beek, M.H., Ferrari, A., Legay, A.: Modelling and analysing ERTMS L3 moving block railway signalling with Simulink and Uppaal SMC. In: Larsen, K.G., Willemse, T. (eds.) FMICS 2019. LNCS, vol. 11687, pp. 1–21. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27008-7_1

17. 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
18. Basile, D., ter Beek, M.H., Legay, A.: Strategy synthesis for autonomous driving in a moving block railway system with Uppaal Stratego. In: Gotsman, A., Sokolova, A. (eds.) FORTE 2020. LNCS, vol. 12136, pp. 3–21. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-50086-3_1
19. Basile, D., Chiaradonna, S., Di Giandomenico, F., Gnesi, S.: A stochastic model-based approach to analyse reliable energy-saving rail road switch heating systems. J. Rail Transp. Plan. Manag. **6**(2), 163–181 (2016). https://doi.org/10.1016/j.jrtpm.2016.03.003
20. Basile, D., Di Giandomenico, F., Gnesi, S.: Statistical model checking of an energy-saving cyber-physical system in the railway domain. In: Proceedings of the 32nd Symposium on Applied Computing (SAC 2017), pp. 1356–1363. ACM (2017). https://doi.org/10.1145/3019612.3019824
21. 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
22. ter Beek, M.H., Borälv, A., Fantechi, A., Ferrari, A., Gnesi, S., Löfving, C., Mazzanti, F.: 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
23. ter Beek, M.H., et al.: Formal methods in industry. Form. Asp. Comput. (2024)
24. ter Beek, M.H., Ciancia, V., Latella, D., Massink, M., Spagnolo, G.O.: Spatial model checking for smart stations: Research challenges. In: Lluch Lafuente, A., Mavridou, A. (eds.) Formal Methods for Industrial Critical Systems. FMICS 2021. LNCS, vol. 12863, pp. 39–47. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-85248-1_3
25. 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
26. Behrmann, G., et al.: UPPAAL 4.0. In: Proceedings of the 3rd International Conference on the Quantitative Evaluation of SysTems (QEST 2006), pp. 125–126. IEEE (2006). https://doi.org/10.1109/QEST.2006.59
27. Belmonte, G., Ciancia, V., Latella, D., Massink, M.: `VoxLogicA`: a spatial model checker for declarative image analysis. In: Vojnar, T., Zhang, L. (eds.) TACAS 2019. LNCS, vol. 11427, pp. 281–298. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17462-0_16
28. Berger, U., James, P., Lawrence, A., Roggenbach, M., Seisenberger, M.: Verification of the European rail traffic management system in real-time Maude. Sci. Comput. Program. **154**, 61–88 (2018). https://doi.org/10.1016/j.scico.2017.10.011
29. Biagi, M., Carnevali, L., Paolieri, M., Vicario, E.: Performability evaluation of the ERTMS/ETCS - level 3. Transp. Res. C-Emerg. **82**, 314–336 (2017). https://doi.org/10.1016/j.trc.2017.07.002
30. Boulanger, J.L.: CENELEC 50128 and IEC 62279 Standards. Wiley, Hoboken (2015)
31. Brooke, J.: SUS: a 'quick and dirty' usability scale. In: Jordan, P.W., Thomas, B., Weerdmeester, B.A., McClelland, I.L. (eds.) Usability Evaluation in Industry, chap. 21, pp. 189–194. CRC press (1996). https://doi.org/10.1201/9781498710411

32. Brooke, J.: SUS: a retrospective. J. Usability Stud. **8**(2), 29–40 (2013). https://doi.org/10.5555/2817912.2817913
33. Broy, M., et al.: Does every computer scientist need to know formal methods? Form. Asp. Comput. (2024)
34. Butler, M., Hoang, T.S., Raschke, A., Reichl, K.: Introduction to the 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
35. Celebi, B.T., Kaymakci, O.T.: Verifying the accuracy of interlocking tables for railway signalling systems using abstract state machines. J. Mod. Transp. **24**(4), 277–283 (2016). https://doi.org/10.1007/s40534-016-0119-1
36. Chiappini, A., et al.: Formalization and validation of a subset of the European train control system. In: Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering (ICSE 2010), vol. 2, pp. 109–118. ACM (2010). https://doi.org/10.1145/1810295.1810312
37. Ciancia, V., Belmonte, G., Latella, D., Massink, M.: A hands-on introduction to spatial model checking using VoxLogicA. In: Laarman, A., Sokolova, A. (eds.) SPIN 2021. LNCS, vol. 12864, pp. 22–41. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-84629-9_2
38. Clark, G., et al.: The Möbius modeling tool. In: Proceedings of the 9th International Workshop on Petri Nets and Performance Models (PNPM 2001), pp. 241–250. IEEE (2001). https://doi.org/10.1109/PNPM.2001.953373
39. Clarke, E.M., Henzinger, T.A., Veith, H., Bloem, R. (eds.): Handbook of Model Checking. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-10575-8
40. Comptier, M., Déharbe, D., Perez, J.M., Mussat, L., Thibaut, P., Sabatier, D.: Safety analysis of a CBTC system: a rigorous approach with Event-B. In: Fantechi, A., Lecomte, T., Romanovsky, A.B. (eds.) RSSRail 2017. LNCS, vol. 10598, pp. 148–159. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-68499-4_10
41. 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
42. 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
43. Dabney, J.B., Harman, T.L.: Mastering Simulink. Pearson, London (2003)
44. DaSilva, C., Dehbonei, B., Mejia, F.: Formal specification in the development of industrial applications: subway speed control system. In: Diaz, M., Groz, R. (eds.) Proceedings of the IFIP TC6/WG6.1 5th International Conference on Formal Description Techniques for Distributed Systems and Communication Protocols (FORTE 1992). IFIP Transactions, vol. C-10, pp. 199–213. North-Holland (1992)
45. David, A., Jensen, P.G., Larsen, K.G., Mikučionis, M., Taankvist, J.H.: Uppaal Stratego. In: Baier, C., Tinelli, C. (eds.) TACAS 2015. LNCS, vol. 9035, pp. 206–211. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46681-0_16
46. David, A., Larsen, K.G., Legay, A., Mikučionis, M., Poulsen, D.B.: Uppaal SMC tutorial. Int. J. Softw. Tools Technol. Transf. **17**(4), 397–415 (2015). https://doi.org/10.1007/s10009-014-0361-y

47. 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
48. 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
49. Dongol, B., et al.: On formal methods thinking in computer science education. Form. Asp. Comput. (2024)
50. 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
51. 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
52. 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
53. Ferrari, A., et al.: Survey on formal methods and tools in railways: the ASTRail approach. In: Collart-Dutilleul, S., Lecomte, T., Romanovsky, A. (eds.) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. RSSRail 2019. LNCS, vol. 11495, pp. 226–241. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-18744-6_15
54. Ferrari, A., Grasso, D., Magnani, G., Fantechi, A., 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
55. 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
56. Ferrari, A., Mazzanti, F., Basile, D., ter Beek, M.H., Fantechi, A.: Comparing formal tools for system design: a judgment study. In: Proceedings of the 42nd ACM/IEEE International Conference on Software Engineering (ICSE 2020), pp. 62–74. ACM (2020). https://doi.org/10.1145/3377811.3380373
57. Fukuda, M., Hirao, Y., Ogino, T.: VDM specification of an interlocking system and a simulator for its validation. IFAC Proc. **33**(9), 187–192 (2000). https://doi.org/10.1016/S1474-6670(17)38144-2. Proceedings of the 9th IFAC Symposium on Control in Transportation Systems (CTS 2000)
58. Furness, N., van Houten, H., Arenas, L., Bartholomeus, M.: ERTMS level 3: the game-changer. IRSE News **232**, 2–9 (2017). https://www.irse.nl/resources/170314-ERTMS-L3-The-gamechanger-from-IRSE-News-Issue-232.pdf
59. Fürst, A., Hoang, T.S., Basin, D.A., Sato, N., Miyazaki, K.: Large-scale system development using abstract data types and refinement. Sci. Comput. Program. **131**, 59–75 (2016). https://doi.org/10.1016/j.scico.2016.04.010
60. 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
61. Guiho, G., Hennebert, C.: SACEM software validation. In: Proceedings of the 12th International Conference on Software Engineering (ICSE 1990), pp. 186–191. IEEE (1990)

62. Hamid, B., Pérez, J.: Supporting pattern-based dependability engineering via model-driven development: approach, tool-support and empirical validation. J. Syst. Softw. **122**, 239–273 (2016). https://doi.org/10.1016/j.jss.2016.09.027
63. 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
64. Hierons, R.M., et al.: Using formal specifications to support testing. ACM Comput. Surv. **41**(2), 9:1–9:76 (2009). https://doi.org/10.1145/1459352.1459354
65. Idani, A., Ledru, Y., Ait Wakrime, A., Ben Ayed, R., Collart-Dutilleul, S.: Incremental development of a safety critical system combining formal methods and DSMLs. In: Larsen, K.G., Willemse, T. (eds.) FMICS 2019. LNCS, vol. 11687, pp. 93–109. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27008-7_6
66. Jaeger, M., Jensen, P.G., Larsen, K.G., Legay, A., Sedwards, S., Taankvist, J.H.: Teaching Stratego to play ball: optimal synthesis for continuous space MDPs. In: Chen, Y.-F., Cheng, C.-H., Esparza, J. (eds.) ATVA 2019. LNCS, vol. 11781, pp. 81–97. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-31784-3_5
67. James, P., Moller, F., Nga, N.H., Roggenbach, M., Schneider, S.A., 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
68. Jifeng, H.: From CSP to hybrid systems. In: Roscoe, A.W. (ed.) A Classical Mind: Essays in Honour of C. A. R. Hoare. Prentice Hall International Series in Computer Science, pp. 171–189. Prentice Hall (1994)
69. Jin, Y., Xie, G., Chen, P., Hei, X., Ji, W., Zhao, J.: High-speed train emergency brake modeling and online identification of time-varying parameters. Math. Probl. Eng. **2020** (2020). https://doi.org/10.1155/2020/3872852
70. Khan, S.A., Zafar, N.A.: Towards the formalization of railway interlocking system using Z-notations. In: Proceedings of the 2nd International Conference on Computer, Control and Communication (IC4 2009), pp. 1–6. IEEE (2009). https://doi.org/10.1109/IC4.2009.4909202
71. Kitchenham, B.: Procedures for performing systematic reviews. Technical report TR/SE-0401, Keele University (2004)
72. Kitchenham, B., Linkman, S., Law, D.: DESMET: a methodology for evaluating software engineering methods and tools. Comput. Control. Eng. J. **8**(3), 120–126 (1997). https://doi.org/10.1049/cce:19970304
73. Kramer, J.: Is abstraction the key to computing? Commun. ACM **50**(4), 36–42 (2007). https://doi.org/10.1145/1232743.1232745
74. Lano, K.: The B Language and Method: a Guide to Practical Formal Development. FACIT. Springer, London (1996). https://doi.org/10.1007/978-1-4471-1494-9
75. Legay, A., Lukina, A., Traonouez, L.M., Yang, J., Smolka, S.A., Grosu, R.: Statistical model checking. In: Steffen, B., Woeginger, G. (eds.) Computing and Software Science. LNCS, vol. 10000, pp. 478–504. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-91908-9_23
76. Leuschel, M., Falampin, J., Fritz, F., Plagge, D.: Automated property verification for large scale B models with ProB. Form. Asp. Comput. **23**(6), 683–709 (2011). https://doi.org/10.1007/s00165-010-0172-1
77. 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

78. 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
79. Mazzanti, F., Ferrari, A., Spagnolo, G.O.: Towards formal methods diversity in railways: an experience report with seven frameworks. Int. J. Softw. Tools Technol. Transf. **20**(3), 263–288 (2018). https://doi.org/10.1007/s10009-018-0488-3
80. Newborn, M.: Automated Theorem Proving. Springer, Germany (2001). https://doi.org/10.1007/978-1-4613-0089-2
81. Petersen, K., Vakkalanka, S., Kuzniarz, L.: Guidelines for conducting systematic mapping studies in software engineering: an update. Inf. Softw. Technol. **64**, 1–18 (2015). https://doi.org/10.1016/j.infsof.2015.03.007
82. Reichl, K., Fischer, T., Tummeltshammer, P.: Using formal methods for verification and validation in railway. In: Aichernig, B.K.K., Furia, C.A.A. (eds.) TAP 2016. LNCS, vol. 9762, pp. 3–13. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-41135-4_1
83. Robinson, J.A., Voronkov, A. (eds.): Handbook of Automated Reasoning. Elsevier, Amsterdam (2001)
84. SAE International: Architecture Analysis & Design Language (AADL) (2022). https://doi.org/10.4271/AS5506D
85. Scupin, R.: The KJ method: a technique for analyzing data derived from Japanese ethnology. Hum. Organ. **56**(2), 233–237 (1997). https://doi.org/10.17730/humo.56.2.x335923511444655
86. 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
87. Snook, C.F., Hoang, T.S., Dghaym, D., Fathabadi, A.S., Butler, M.J.: Domain-specific scenarios for refinement-based methods. J. Syst. Archit. **112** (2021). https://doi.org/10.1016/j.sysarc.2020.101833
88. 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
89. Wang, S., Zhan, N., Zou, L.: An improved HHL prover: an interactive theorem prover for hybrid systems. In: Butler, M., Conchon, S., Zaïdi, F. (eds.) ICFEM 2015. LNCS, vol. 9407, pp. 382–399. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25423-4_25
90. Wang, Y., Chen, L., Kirkwood, D., Fu, P., Lv, J., Roberts, C.: Hybrid online model-based testing for communication-based train control systems. IEEE Intell. Transp. Syst. Mag. **10**(3), 35–47 (2018). https://doi.org/10.1109/MITS.2018.2842230
91. Wu, D., Schnieder, E.: Scenario-based system design with colored Petri nets: an application to train control systems. Softw. Syst. Model. **17**(1), 295–317 (2018). https://doi.org/10.1007/s10270-016-0517-1
92. Zhan, B., et al.: Compositional verification of interacting systems using event monads. In: Andronick, J., de Moura, L. (eds.) Proceedings of the 13th International Conference on Interactive Theorem Proving (ITP 2022). LIPIcs, vol. 237, pp. 33:1–33:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2022). https://doi.org/10.4230/LIPIcs.ITP.2022.33