On the Industrial Uptake of Formal Methods in the Railway Domain

A Survey with Stakeholders

Davide Basile[1,3], Maurice H. ter Beek[1], Alessandro Fantechi[1,3]
Stefania Gnesi[1], Franco Mazzanti[1],
Andrea Piattino[2], Daniele Trentini[2], and Alessio Ferrari[1]

[1] ISTI–CNR, Pisa, Italy
{basile,terbeek,alessio.ferrari,gnesi,mazzanti}@isti.cnr.it
[2] SIRTI S.p.A., Italy
{a.piattino,d.trentini}@sirti.it
[3] Università di Firenze, Italy
alessandro.fantechi@unifi.it

Abstract. The railway sector has seen a large number of successful applications of formal methods and tools. However, up-to-date, structured information about the industrial usage and needs related to formal tools in railways is limited. As a first step to address this, we present the results of a questionnaire submitted to 44 stakeholders with experience in the application of formal tools in railways. The questionnaire was oriented to gather information about industrial projects, and about the functional and quality features that a formal tool should have to be successfully applied in railways. The results show that the most used tools are, as expected, those of the B family, followed by an extensive list of about 40 tools, each one used by few respondents only, indicating a rich, yet scattered, landscape. The most desired features concern formal verification, maturity, learnability, quality of documentation, and ease of integration in a CENELEC process. This paper extends the body of knowledge on formal methods applications in the railway industry, and contributes with a ranked list of tool features considered relevant by railway stakeholders.

1 Introduction

The railway field is known for its robust safety requirements and its rigorous development processes. In fact, formal methods and tools have been widely applied to the development of railway systems during the last decades (cf., e.g., [1, 2, 4–7, 9, 11–17, 21–24]) and the CENELEC EN 50128 standard for the development of software for railway control and protection systems mentions formal methods as highly recommended practices for SIL 3–4 platforms [8, 10]. The extensive survey on formal methods applications by Woodcock et al. [25], which included a structured questionnaire submitted to the participants of 56 projects, also identified the transport domain, including railways, as the one in which the largest number of projects including applications of formal methods has been performed. Relevant examples are the usage of the B method for developing railway signalling systems in France, like, e.g., Line 14 of the Paris Métro and the driverless Paris Roissy Airport shuttle [1]. Another is the usage of Simulink/Stateflow for formal model-based development, code generation, model based-testing and abstract interpretation in the development of the Metrô Rio ATP system [11]. Many projects have been also carried out, often in collaboration with national railway companies, for the verification of interlocking systems [13, 20–24].

Despite this long tradition and history, no universally accepted formal method or tool has emerged. Thus, on the one hand, railway companies wishing to introduce formal methods have little guidance for the selection of the most appropriate formal methods to use to develop their systems. On the other hand, tool vendors lack a clear reference concerning the features that are relevant for users of a tool in the railway domain. This paper aims to provide a first contribution to address these issues by presenting the results of a questionnaire submitted to experts in the theory and practice of formal methods in railways. The questionnaire's goal is to: (a) show the trends in the application of formal methods to railway systems, and (b) identify the most relevant features that a tool should support to be applied in railway systems' development.

This work is the first output of a larger endeavour that the authors are performing in the context of the ASTRail EU project[4] (SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block Validation), funded by EU's Shift2Rail initiative[5]. A specific work stream of the project is concerned with an assessment of the suitability of formal methods in supporting the transition to the next generation of ERTMS/ETCS signalling systems [2–4]. The work stream's roadmap follows the two phases:

1. An *analysis* phase dedicated to survey, compare and evaluate the main formal methods and tools currently used in the railway industry.
2. An *application* phase in which selected formal methods are used to model and analyse two main goals of the project (moving block distancing and automatic driving) to validate that the methods not only guarantee safety, but also, more in general, the software's long-term reliability and availability.

The work presented in this paper is part of the analysis phase of ASTRail, in which the information retrieved with the questionnaire will be complemented with a systematic literature review and a systematic tool trial. Based on these tasks, we aim to complement the survey of Woodcock et al. [25] with a specific, in-depth focus on railway applications.

The paper is structured as follows: In Section 2, we provide information about the criteria used to define the questionnaire, and afterwards we present its results in Section 3. In Section 4, we provide conclusions and final remarks.

[4] http://astrail.eu

[5] http://shift2rail.org

2 Questionnaire Definition

For the nontrivial task of obtaining a significative amount of data from industrial stakeholders, a survey was carried out by means of a structured questionnaire, submitted to the participants of the recent RSSRail'17 conference[6]. This venue is attended by academics and practitioners interested in applying formal methods in railways, and as such a promising source for a population sample that might be able to provide a well-informed judgement.

The goal of the questionnaire was to: (a) identify the current uptake of formal and semi-formal methods and tools in the railway sector; (b) identify the features, in terms of functional and quality aspects, that are considered more relevant for the application of a certain formal tool in the development of railway products. The questionnaire was designed to be easy to understand by the target group, involving academics and practitioners, and to be filled within five minutes, to limit the amount of time required for the people surveyed, and possibly increase the number of respondents. The design of the questionnaire was performed by the authors of the current paper, who include both academics with expertise in formal methods applied to railways and practitioners from railway industry. For the questions concerning the relevance of the tool features (cf. Section 3.3), a two-hour brainstorming session based on the KJ-method [18] was organised to identify possibly relevant features. The questionnaire was tested and validated with industrial partners of the ASTRail consortium for clarity and the time required. An online version of the questionnaire, which the reader can refer to have a clear view of the proposed questions, can be found at the following link: https://goo.gl/forms/4b9wSTJAMOK7VghW2.

3 Results of the Questionnaire

In the following sections, we report and interpret the results that we obtained.

3.1 Affiliations and Experience

The first part of the questionnaire was dedicated to identify the respondents in terms of affiliation and experience in railways and formal/semi-formal methods and tools. The 44 respondents are balanced between academics (50%) and practitioners (50%, of which 47.7% from railway companies and 2.3% from aerospace and defense). A large percentage of respondents has several years of experience in railways (68% more than 3 years and 39% more than 10 years) and in formal methods (75% more than 3 years, 52% more than 10 years), and this confirms that our sample can provide informed opinions on the proposed questions[7].

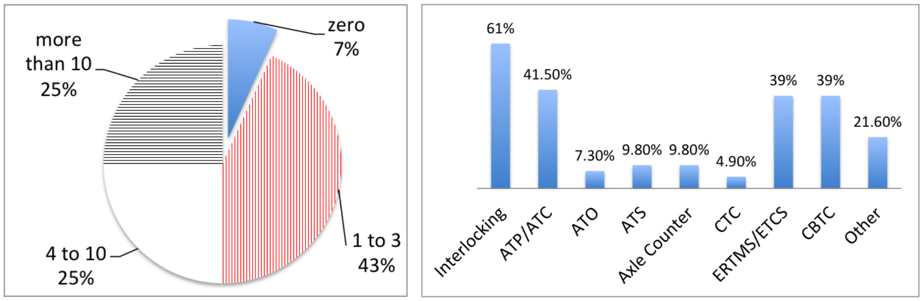
[6] http://conferences.ncl.ac.uk/rssrail/

[7] We did not weigh the results based on the declared experience of the respondents, because we wanted to give equal importance to their different answers, regardless of the specific experience.

3.2 Usage of Formal Methods in Railway Sector

The second part of the questionnaire was oriented to have an insight on the usage of formal/semi-formal methods and tools in railways.

Projects We asked in how many *industrial* railway projects the respondents, or their teams, have used formal/semi-formal methods and tools. Since the respondents included also academics, we expected that the industrial projects in which they were involved were mainly technology transfer projects with companies. Figure 1a shows that only 7% of the respondents—or their teams—did not have any industrial experience in the application of formal methods in railways[8].



(a) Number of projects

(b) Type of products

Fig. 1: Usage of formal methods in the railway sector

Products Figure 1b shows the main types of products developed with the support of formal methods. The cited systems include an extensive range of signalling systems and components. The majority of the respondents applied formal methods to interlocking systems (61% of the respondents[9]), but also automatic train protection/automatic train control (ATP/ATC) distancing systems (41.5%), especially in their standardised form for main lines (ERTMS/ETCS, 39%) or for metro lines (CBTC, 39%) play a major role. Automatic train operation (ATO), automatic train supervision (ATS), axle counter systems and centralised traffic control (CTC) are also mentioned. This prominence of in particular interlocking and ATP/ATC systems is in line with the formal methods literature, for which these types of systems are traditional applications [9].

Phases With the aim of estimating the degree of integration of formal methods in software engineering practice, respondents were asked to indicate the phase of the development process in which formal methods are applied (cf. Figure 2). We see that all phases have been selected by at least one of the respondents, highlighting the potential pervasiveness of formal methods within the development process.

[8] When present, the subsequent answers of these respondents were discarded from our statistics, since they were considered outliers with respect to our population sample.

[9] For this and subsequent questions, respondents could select more than one answer.

Most of the respondents (73.8%) used them for specification and formal verification. Also analysis of specifications (50%) and simulation (40.5%) appear to be common, and a non-negligible amount of respondents (31%) used formal methods also within model-based testing and code generation contexts. Less common (7.1%) is their application to the static analysis of the source code.

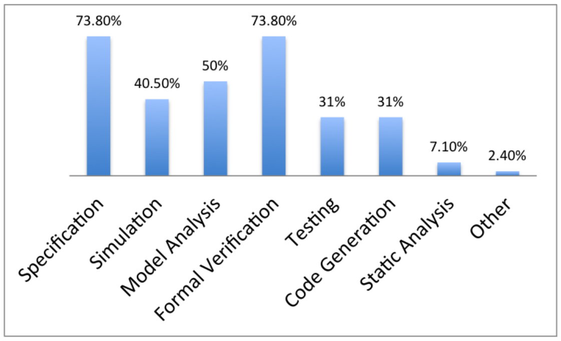


Fig. 2: Phase of the process in which formal methods are applied

Tools The respondents were also asked to list the tools they have used in the context of their projects, and, in this case, we believe it is interesting to separate the results of industrial respondents from those of academics. In Figure 3, we can see that the large majority of industrial and academic respondents mentioned tools belonging to the B method family (e.g. B, ProB, AtelierB, EventB, RODIN). The relationship between the B method and the railway sector is well established: as Sun [19] puts it, "the B proved models are considered *safe* in French industry." Actually, there are only slightly more industrial users than academic users in our sample, but we recall that the academic users were asked to report on their collaborative projects with industry. Other methods and tools mentioned by both groups are the Matlab toolsuite—including Simulink and Stateflow—SCADE, Petri nets/CPN tools and Monte Carlo Simulation: the overlapping between tools used in industry and in academia is actually limited to these five elements. Industrial users named a few other tools as well, whereas a large list of other tools has been named by academics, with popular model checkers like NuSMV and SPIN leading this list. An interpretation of this can be that a frequent pattern of collaboration between academia and industry includes the academic support in adopting advanced formal verification techniques inside a collaborative project.

3.3 Feature Relevance

The final part of the questionnaire was dedicated to identify the most relevant features that a formal/semi-formal tool should have to be used in the railway industry. Features are partitioned into supported functional and quality aspects. We asked to check at most three relevant functional features, among the seven listed, and at most five relevant quality aspects, among the sixteen listed.

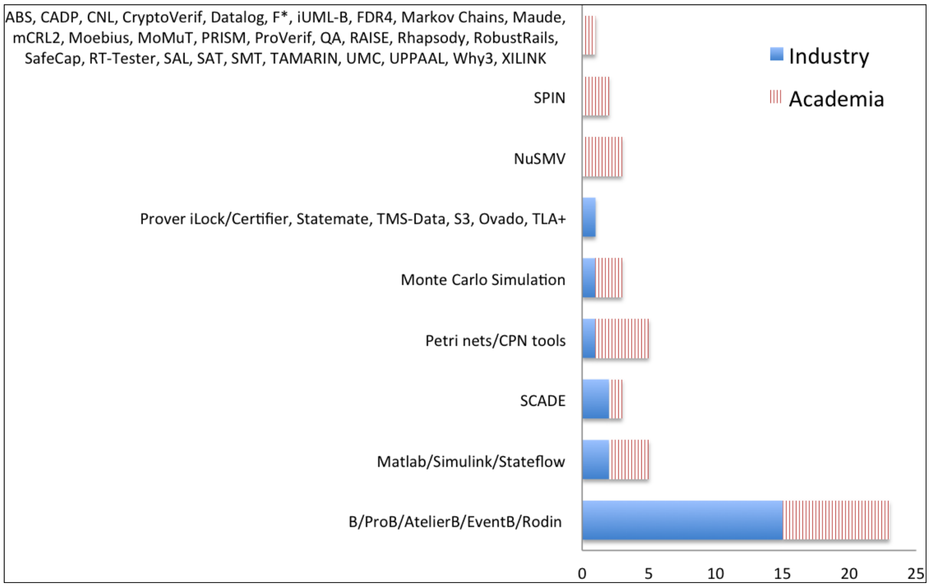


Fig. 3: Tools cited in the questionnaire

Functional features Figure 4 shows the results for the most relevant functional features. All the listed features are considered relevant by at least one of the respondents. The functional features that are considered most relevant by the majority of the respondents are formal verification (86.4% of the respondents), followed by modelling—graphical or textual—(72.7%). These traditional functional features of formal tools are followed by simulation (30%) and traceability (27.3%). Indeed, simulation (often in the form of animation of a graphical specification) is needed for a quick check of the behaviour of a model; traceability

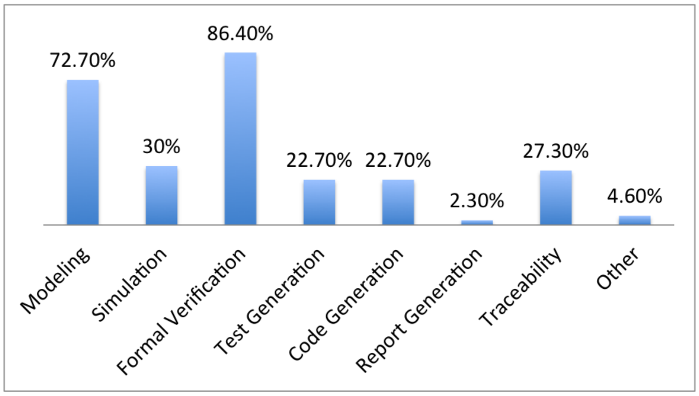


Fig. 4: The most relevant functional features a (semi-)formal tool should support

between the artefacts of the software development (requirements to/from models, models to/from code, etc.) is mandatorily required by the main guidelines for the development of safety-critical systems. Functional features, such as test generation and code generation, related to later activities of the development process, are also considered relevant by a non-negligible amount of respondents (22.7%). These numbers suggest that formal tools are seen to play a role mostly in the early phases of the development process, for specification and formal verification. These are also the phases in which formal methods cannot be substituted by any other means—while this may happen in testing, code development and tracing.

Quality aspects Figure 5, finally, reports the most relevant quality aspects and, also in this case, all the listed answers were checked by at least one of the respondents. The maturity of the tool (stability and industry readiness) is considered to be among the most relevant quality aspects by 75% of the respondents, followed by learnability by a railway software developer (45.5%), quality of documentation (43.2%) and ease of integration in the CENELEC process (36.4%). Overall, the most relevant quality aspects are associated to the usability of the tool. Less relevant are deployment aspects, such as platforms supported (9.1%) and flexible license management (11.4%). Interestingly, also the low cost of the tool (13.6%) appears to be a not extremely relevant feature. This is a reasonable finding. Indeed, the development and certification cost of railway products is high and, hence, if a company expects to reduce these costs through a formal tool, it can certainly tolerate the investment on the tool.

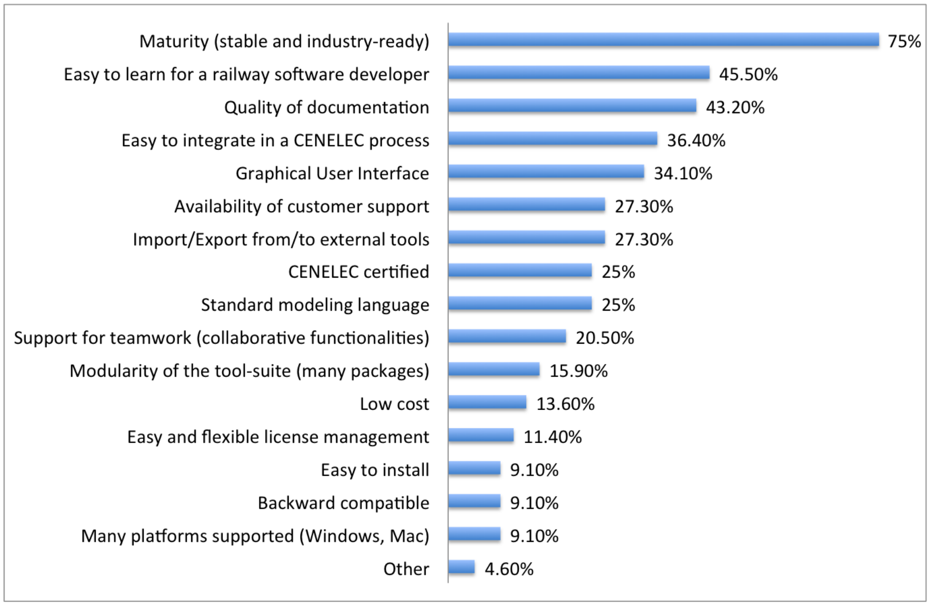


Fig. 5: The most relevant quality aspects a (semi-)formal tool should have

3.4 Threats to Validity

Concerning construct and internal validity, the questions defined and the options proposed as answers may be incomplete to identify practical uses of tools, and desired features. Furthermore, the respondents may have misunderstood the meaning of the questions. To mitigate these threats, the questions were designed and tested in collaboration between academic and industrial partners.

Concerning statistical conclusion validity, we do not have an estimate of the whole population of subjects applying formal methods in railways, and our sample was limited to the participants of RSSRail. However, assuming that the population of persons applying formal methods in railways is $1,000$, our results on a sample of 44 persons are valid for a confidence level of 85% and margin of error of 10.5%. While higher values are normally targeted in qualitative research, the answers to the questionnaire show that the sample is made of high-quality (i.e. informed) respondents, which increases the reliability of our results. However, we cannot exclude that important industrial applications of formal methods are not public, and people working on them may not attend conferences like RSSRail, for confidentiality policies.

4 Conclusion

Formal methods and tools have been applied quite extensively in specific industrial domains, especially those in which safety-critical software is produced, either in pilot projects or in daily production. On the other hand, industry often confronts itself with the choice among a large variety of techniques and tools, with little help for selecting the ones that better fit their needs. Within the H2020 ASTRail project, the authors are working on providing information to guide railway practitioners interested in the adoption of formal methods.

To this end, we performed the questionnaire presented in this paper and we are working on a literature survey on formal methods for railways, as well as on a systematic tool evaluation (cf. [14, 16] for preliminary comparisons of formal modelling and verification frameworks). The current work provides preliminary information on the industrial uptake of formal methods in railways. The results show that, although the B method appears to be the one that is mostly used in the railway industry, several other tools have been used, and some of them are not even considered by the academics that were part of the respondents. Furthermore, we observed that industrial needs concerning formal tools are mostly related to usability features, such as maturity of the tools, learnability, and quality of documentation. Interestingly, the cost of the tools is not a highly relevant issue, suggesting that industry appears to be available to invest in formal tools, if these guarantee a process cost reduction and the expected safety assurance.

Acknowledgements This work has been partially funded by the ASTRail project. This project received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No. 777561.

References

1. Abrial, J.R.: Formal Methods: Theory Becoming Practice. J. Univers. Comput. Sci. **13**(5), 619–628 (2007). https://doi.org/10.3217/jucs-013-05-0619
2. 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.) Proceedings of the 8th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA 2018). LNCS, Springer, Germany (2018), to appear
3. ter Beek, M.H., Fantechi, A., Ferrari, A., Gnesi, S., Scopigno, R.: Formal Methods for the Railway Sector. ERCIM News **112**, 44–45 (2018), https://ercim-news.ercim.eu/en112/r-i/formal-methods-for-the-railway-sector
4. ter Beek, M.H., Fantechi, A., Gnesi, S.: Product line models of large cyber-physical systems: the case of ERTMS/ETCS. In: Proceedings of the 22nd International Systems and Software Product Line Conference (SPLC 2018). ACM, USA (2018). https://doi.org/10.1145/3233027.3233046
5. 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
6. Bjørner, D.: New Results and Trends in Formal Techniques and Tools for the Development of Software for Transportation Systems — A Review. In: Tarnai, G., Schnieder, E. (eds.) Proceedings of the 4th Symposium on Formal Methods for Railway Operation and Control Systems (FORMS 2003). L'Harmattan, Hungary (2003)
7. Boulanger, J.L. (ed.): Formal Methods Applied to Industrial Complex Systems — Implementation of the B Method. John Wiley & Sons, USA (2014). https://doi.org/10.1002/9781119002727
8. European Committee for Electrotechnical Standardization: CENELEC EN 50128 — Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems (1 June 2011), https://standards.globalspec.com/std/1678027/cenelec-en-50128
9. Fantechi, A.: Twenty-Five Years of Formal Methods and Railways: What Next? In: Counsell, S., Núñez, M. (eds.) Software Engineering and Formal Methods — Revised Selected Papers of the SEFM 2013 Collocated Workshops: BEAT2, WS-FMDS, FM-RAIL-Bok, MoKMaSD, and OpenCert. LNCS, vol. 8368, pp. 167–183. Springer, Germany (2013). https://doi.org/10.1007/978-3-319-05032-4_13
10. Fantechi, A., Ferrari, A., Gnesi, S.: Formal Methods and Safety Certification: Challenges in the Railways Domain. In: Margaria, T., Steffen, B. (eds.) Proceedings of the 7th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications (ISoLA 2016). LNCS, vol. 9953, pp. 261–265. Springer, Germany (2016). https://doi.org/10.1007/978-3-319-47169-3_18
11. 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
12. Flammini, F. (ed.): Railway Safety, Reliability, and Security: Technologies and Systems Engineering. IGI Global, USA (2012). https://doi.org/10.4018/978-1-4666-1643-1
13. James, P., Moller, F., Nguyen, H.N., Roggenbach, M., Schneider, S., Treharne, H.: Techniques for modelling and verifying railway interlockings. Int. J. Softw. Tools Technol. Transf. **16**, 685–711 (2014). https://doi.org/10.1007/s10009-014-0304-7

14. Mazzanti, F., Ferrari, A.: Ten Diverse Formal Models for a CBTC Automatic Train Supervision System. In: Gallagher, J.P., van Glabbeek, R., Serwe, W. (eds.) Proceedings of the 3rd Workshop on Models for Formal Analysis of Real Systems and the 6th International Workshop on Verification and Program Transformation (MARS/VPT 2018). Electronic Proceedings in Theoretical Computer Science, vol. 268, pp. 104–149 (2018). https://doi.org/10.4204/EPTCS.268.4
15. 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
16. Mazzanti, F., Spagnolo, G.O., Longa, S.D., Ferrari, A.: Deadlock Avoidance in Train Scheduling: A Model Checking Approach. In: Lang, F., Flammini, F. (eds.) Proceedings of the 19th International Conference on Formal Methods for Industrial Critical Systems (FMICS 2014). LNCS, vol. 8718, pp. 109–123. Springer, Germany (2014). https://doi.org/10.1007/978-3-319-10702-8
17. Moller, F., Nguyen, H.N., Roggenbach, M., Schneider, S., Treharne, H.: Defining and Model Checking Abstractions of Complex Railway Models Using CSP||B. In: Biere, A., Nahir, A., Vos, T. (eds.) Hardware and Software: Verification and Testing —Revised Selected Papers of the 8th International Haifa Verification Conference (HVC 2012). LNCS, vol. 7857, pp. 193–208. Springer, Germany (2013). https://doi.org/10.1007/978-3-642-39611-3_20
18. 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
19. Sun, P.: Model based system engineering for safety of railway critical systems. Ph.D. thesis, Ecole Centrale de Lille (2015), https://tel.archives-ouvertes.fr/tel-01293395
20. Vanit-Anunchai, S.: Modelling and simulating a Thai railway signalling system using Coloured Petri Nets. Int. J. Softw. Tools Technol. Transf. **20**(3), 243–262 (2018). https://doi.org/10.1007/s10009-018-0482-9
21. Vu, L.H., 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
22. Winter, K.: Model Checking Railway Interlocking Systems. In: Oudshoorn, M.J. (ed.) Proceedings of the 25th Australasian Conference on Computer Science (ACSC 2002). Conferences in Research and Practice in Information Technology, vol. 4, pp. 303–310. Australian Computer Society, Australia (2002), http://crpit.com/confpapers/CRPITV4Winter.pdf
23. Winter, K., Johnston, W., Robinson, P., Strooper, P., van den Berg, L.: Tool support for checking railway interlocking designs. In: Cant, T. (ed.) Proceedings of the 10th Australian Workshop on Safety Critical Systems and Software (SCS 2005). Conferences in Research and Practice in Information Technology, vol. 55, pp. 101–107. Australian Computer Society, Australia (2006), http://crpit.com/confpapers/CRPITV55Winter.pdf
24. Winter, K., Robinson, N.J.: Modelling large railway interlockings and model checking small ones. In: Oudshoorn, M.J. (ed.) Proceedings of the 26th Australasian Computer Science Conference (ACSC 2003). Conferences in Research and Practice in Information Technology, vol. 16, pp. 309–316. Australian Computer Society, Australia (2003), http://crpit.com/confpapers/CRPITV16Winter.pdf
25. Woodcock, J., Larsen, P.G., Bicarregui, J., Fitzgerald, J.S.: Formal methods: Practice and experience. ACM Comput. Surv. **41**(4), 19:1–19:36 (2009). https://doi.org/10.1145/1592434.1592436