Adopting Formal Methods in an Industrial Setting: The Railways Case

Maurice H. ter Beek[1], Arne Borälv[3], Alessandro Fantechi[1,2], Alessio Ferrari[1], Stefania Gnesi[1], Christer Löfving[3], and Franco Mazzanti[1]

[1] ISTI–CNR, Pisa, Italy
{terbeek,ferrari,gnesi,mazzanti}@isti.cnr.it
[2] Università di Firenze, Italy
alessandro.fantechi@unifi.it
[3] Trafikverket, Sweden
christer.lofving@trafikverket.se

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. Two Shift2Rail projects, X2Rail-2 and ASTRail, have addressed this issue by performing a systematic search over the state of the art of formal methods application in railways to identify the best used practices. As part of the work of these projects, questionnaires on formal methods and tools have been designed to gather input and guidance on the adoption of formal methods in the railway domain. Even though the questionnaires were developed independently and distributed to different audiences, the responses show a certain convergence in the replies to the questions common to both. In this paper, we present a detailed report on such convergence, drawing some indications about methods and tools that are considered to constitute the most fruitful approaches to industrial adoption.

1 Introduction

The benefits that can be expected from using formal methods depend on several factors and can vary considerably depending on the scope and purpose, the quality and maturity of the tools that are used, the knowledge of users of the formal methods and tools, and so on.

Considering *formal specification* of requirements, formal methods provide a better insight and understanding, compared to specifying requirements in natural language. Formal specifications may be processed automatically by software tools, allowing the requirements to be debugged during development. Besides such benefits, a formal specification can be used as basis to prove that a system (model) satisfies its requirements using formal verification.

Formal verification enables exhaustive verification that critical properties related to safety and security are satisfied, which traditional methods based on test and simulation cannot. This makes it possible to accurately identify meaningful errors, and to provide strong guarantees for correctness. In addition, formal verification is often (but not always) automated which can reduce the

effort and time for proving the correctness of systems considerably. In the last decade or two, formal verification has matured considerably, thanks to more sophisticated algorithms for formal verification and more powerful computers.

The largest benefits can be expected from *formal development*, that is, integrating formal methods in the development process, so that safer software can be produced with lower costs. Formal development may replace existing processes, but this requires a large commitment and investment, including a learning curve to become proficient in a new process.

Successful applications of formal methods in industry (automotive, avionics, etc.) have demonstrated these benefits to varying degree, and have shown that the number of defects in the code can be significantly reduced [1,4,10,11]. However, formal methods do not pervade critical software industry, and this happens also in the railway domain, despite several success stories [3,6,7] and even though formal methods are highly recommended by the CENELEC standards [5].

The Shift2Rail Joint Undertaking (S2R JU) has identified the use of formal methods as one of the key concepts to enable reducing the time it takes to develop and deliver railway signalling systems, and to reduce high costs for procurement, development and maintenance. formal methods have been recognized as needed to ensure correct behaviour, interoperability and safety, at the same time reducing long-term life cycle costs. In this S2R JU initiative, two complementary projects, one proposed by the JU Members themselves, the other one as a result of an open call, respectively X2Rail-2[4] and ASTRail[5], have been funded having as one of the objectives common to both, that is, to perform a search over the state of the art of formal methods application in railways to identify the best used practices. As part of the work of the two projects, questionnaires on formal methods and tools have been designed to gather input and guidance on the adoption of formal methods in the railway domain. The purpose was to validate existing know-how and experience in the subject matter and to gain insight into expectations by the railway industry regarding what formal methods can and should bring. Even though the questionnaires were developed independently and distributed to different audiences by the two projects, the responses show a certain convergence in the replies to the questions common to both.

In this paper, we present a detailed report on such convergence, drawing some indications about methods and tools that are considered to constitute the most fruitful approaches to industrial adoption. Indeed, the main aim of the questionnaires was, in both cases, to investigate:

- The most relevant functionality of formal methods applications among, e.g., formal verification, requirement traceability, test case generation and simulation, etc.
- The system development phases that can benefit most from using formal tools.
- The most important quality aspect of formal tools, such as maturity, easy to learn, easy to integrate in a CENELEC process, etc.

[4] https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-2
[5] http://www.astrail.eu

This paper is organized as follows: the questionnaires are presented in Sect. 2. The results of the questionnaires are shown in Sect. 3, after an elaboration aimed to cumulate and harmonize the raw results of the different questionnaires. Lessons learned and conclusions are summarized in Sect. 4.

2 Questionnaires

Three questionnaires were defined, two by the X2Rail-2 project [12] and one by the ASTRail project [2,8]. In the following, we will distinguish them by the names X2Rail2-a, X2Rail2-b and ASTRail.

The questionnaires were independently distributed to different audiences by the two projects in order to gather feedback on the usage of formal methods in the railway domain, both from academic and industrial stakeholders. Below we summarize the main characteristics of the respondents.

***X2Rail2-a*:**
- 17 out of 22 invited individuals answered the questionnaire.
- The respondents had on average 10 years of experience in railway signalling and 9 years in formal methods.
- One third of the respondents were affiliated with a supplier company, one third with a research institution, and one quarter were from an infrastructure manager.
- Most respondents had experience from projects using formal methods, with such projects delivering systems in revenue service or as pilots.
- The most common signalling subsystem type of such projects has been interlocking, followed by on-board software.

***X2Rail2-b*:**
- 86 out of 500 invited individuals answered the questionnaire.
- The respondents had on average 20 years of experience in railway signalling.
- 38% of the respondents were affiliated with an infrastructure manager, 16% with a supplier company, 28% with engineering firms, 5% with a research institution, and 5% with safety assessment.
- More than half of the respondents were familiar with formal methods for development of railway signalling systems (formal specification, formal verification, semi-formal methods).
- More than half of the respondents had used formal methods (directly or indirectly).

***ASTRail*:**
- The questionnaire was proposed to the participants of the RSSRail'17 conference. The 44 respondents were 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 had 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).

3 Cumulated Results of the Two Projects' Questionnaires

In order to extend the validity of the results obtained by the different questionnaires, we considered the integration of their results, focusing on those questions that are common, or similar, between them. Even in the case of the same or similar questions, sometimes the questionnaires proposed a different set of closed form replies: this required a harmonization effort which in some case has necessarily reduced the information provided by one of the questionnaires.

Products Both projects included questions on the type of railway signalling systems to which formal methods were applied by respondents or their institution; however, X2Rail2-a also distinguished between equipments belonging to ERTMS, CBTC or conventional signaling applications. Figure 1 shows a summary of the results expressed as the percentage of the respondents to ASTRail, while for X2Rail2-a the percentages are given for each application category (multiple answers were allowed, so the sum is not 100).

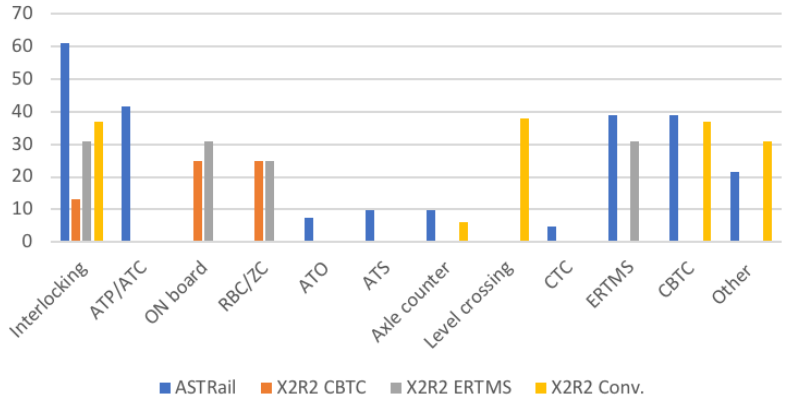

Fig. 1: Usage of formal methods in the railway sector – Type of Products

Phases Another common question of ASTRail and X2Rail2-a regarded the phases of the development process in which formal methods were applied. Unfortunately, the two questionnaires proposed a different granularity in the definition of the phases, and we were therefore unable to meaningfully synthesize the results beyond the mere juxtaposition presented in Table 1, in which the location of the entries hints at some rough correspondences between the two cases, and where the numbers give the percentage of interested respondents for each questionnaire.

Formal Tools Tools based on formal methods, for short *formal tools*, have been the key to success stories of industrial application of formal methods [9, 11]. The questionnaires therefore addressed the industrial diffusion of formal tools, without providing any specific list of tools in advance, nor any predefined definition of what constitutes a formal tool. ASTRail and X2Rail2-a differ for the

Table 1: Phases in the process in which formal methods are applied

Phase	***ASTRail***	***X2Rail2-a***
Specification	73.8	
User Requirements		6
Prototyping		13
System Level User Requirements		31
Software User Requirements		69
System configuration		13
Design		63
Simulation	40.5	
Model analysis	50.0	
Formal verification	73.8	
Design verification		50
Code Generation	32.0	
Coding		38
Testing	32.0	
Code verification		25
Unit testing		25
Integration testing		13
Static analysis	7.1	
Safety Assessment		19
Other	2.4	13

classification of used tools (X2Rail2-b did not include a question asking for tool identification):

- In X2Rail2-a there are separate questions related to formal verification, formal specification and formal development.
- In ASTRail only the name of used tools where asked, irrespective of the phase in which they were used.

To harmonize the results, we ignored the phase distinction made in X2Rail2-a: we simply merged the three values given by respondents to X2Rail2-a by assuming that who has indicated the use of a tool in a phase is one of those that indicated the use of the same tool for another phase, that is, it is more likely that someone adopting a tool for one phase has adopted the same tool for another phase. Under this assumption, for each tool we took the maximum of the numbers of users given for each phase. Moreover, to simplify the presentation, we merged values related to tools that form the *B ecosystem*, merged values referring to Petri Net tools and removed from X2Rail2-a the answers on semi-formal tools (cf. next paragraph). We then ordered the tools in Fig. 2 by the sum of the resulting ASTRail and X2Rail2-a values, removing all tools mentioned only once in one of the questionnaires, in order to contain the size of the figure.[6]

[6] The list of tools gaining only one mention is: ABS, Astah, CADP, CNL, CryptoVerif, Datalog, F*, iUML-B, FDR4, Markov Chains, Maude, mCRL2, Moebius, MoMuT,

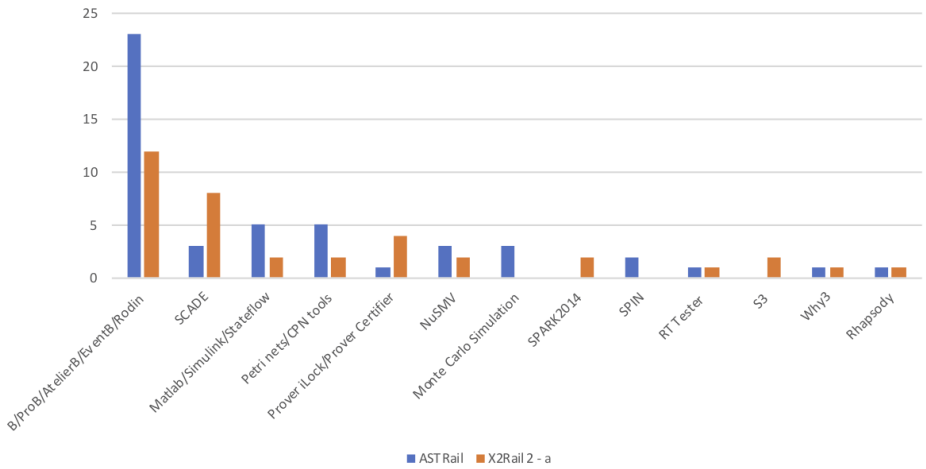

Fig. 2: Tools cited in the questionnaires

We notice that the industrial perception of what constitutes a formal method or a formal tool is rather liberal, including some tools and languages that may not be considered 'formal' according to canonical definitions of formal methods. For example, typical commercial *model-based design* tools like SCADE and Simulink were cited among tools offering formal verification capabilities, and therefore in this respect are considered formal. In line with [9], we extend this liberal notion of formal tools to Rhapsody as well (in spite of what will be said later about UML) since, although not offering formal verification, it provides simulation and automatic test generation capabilities to support the design, construction and analysis of systems. Moreover, such features are considered among the most relevant ones requested from formal tools, as we will show later in Fig. 4. On the other hand, respondents also listed generic names of verification techniques (SAT, Monte Carlo simulation, etc.) rather than specific tools.

Semi-formal Tools Semi-formal methods refer to formalisms and languages that are not considered fully 'formal'. Examples include UML and dialects thereof, in which requirements are expressed using graphical diagrams. Although semi-formal, such diagrams can convey the meaning of requirements more clearly than natural language. Advocates consider the use of semi-formal methods worthwhile, for instance due to easier adoption during earlier phases such as when defining and eliciting the user and system requirements. Using semi-formal methods simply defers the task of completing the semantics to a later stage. Semi-formal tools were cited only in X2Rail2-a, whose results are reported in Fig. 3.

PRISM, ProVerif, QA, RAISE, RobustRails, SafeCap, SAL, SAT, SMT, TAMARIN, UMC, UPPAAL, and XILINK.

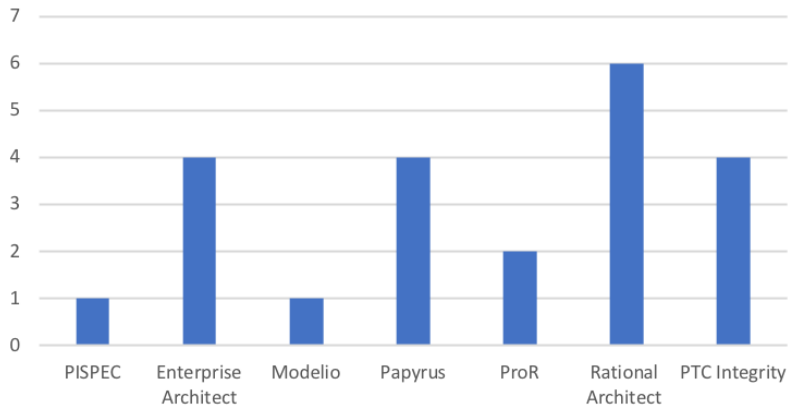

Fig. 3: Semi-formal tools

Figures 2 and 3 already show a convergence towards a limited set of tools. This trend is even more marked if we cross these results with those coming from other sources, that is, the systematic literature review conducted in the ASTRail project, and the associated study of European industrial research projects related to the application of formal methods in railway signalling [2, 8].

Expectations on Tools The respondents to all three questionnaires were asked, according to their experience, what they considered to be the most relevant functionalities that formal (or semi-formal) methods and tools should support. Figure 4 depicts the compared results, which exhibit a substantial agreement: verification is by far the functionality that is asked most from a formal tool.

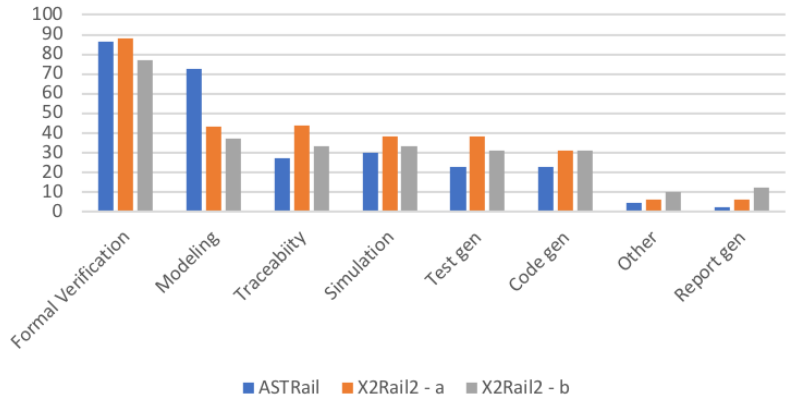

Fig. 4: Most relevant features

Another question common to the three questionnaires concerns the most relevant quality aspects that (semi-)formal tools should have in order to be used in the railway industry. The results depicted in Fig. 5 show that maturity,

easy learning and easy integration in a CENELEC development process are the qualities that scored highest. We note that ASTRail and X2Rail2-b show a more substantial agreement, while X2Rail2-a scores differently some aspects (e.g., the importance of the tools' cost).

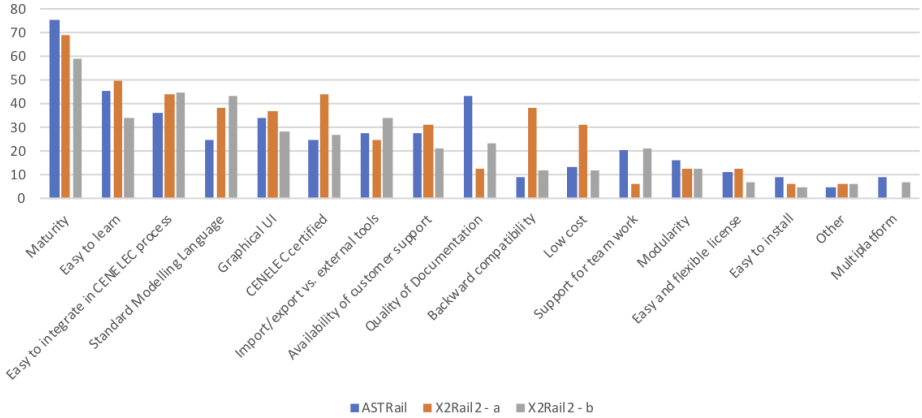

Fig. 5: Relevant quality aspects

4 Conclusion

Formal methods have been largely applied to railway problems for more than three decades. However, structured information is limited about their current application in industry, and about the most relevant features that practitioners expect from tools supporting formal development. In this paper, we merge the information elicited through three different questionnaires involving practitioners and academics with experience in formal methods and railway systems. The questionnaires were performed in the contexts of two ongoing Horizon 2020 research projects funded through the Shift2Rail initiative, namely ASTRail and X2Rail-2. Both projects include tasks specifically dedicated to collect information about the application of formal methods in railways. The results of the questionnaires show the following:

1. Most of the applications of formal methods in industrial projects are focused on interlocking systems.
2. Formal methods are mainly used for formal specification and formal verification, mostly in the early development phases, as requirements and design.
3. The B-family is the dominant set of tools, followed by tools with simulation capabilities such as SCADE and Simulink.
4. The most relevant functionalities are formal verification and support for formal modelling, followed by traceability, simulation, test and code generation.
5. The most relevant quality features are related to the maturity, usability and learnability of the tools.

This paper consolidates the body of knowledge in formal methods for railway system development by confirming some trends (e.g., dominance of the B-method, focus on early development phases) that are visible to the interested practitioners and academics, by means of an empirical inquiry. The conducted study has also shown a certain gap in the industrial perception of what formal methods and tools are, with respect to more canonical definitions of these terms.

There is an obvious threat to the validity of the conclusions of this work, due to the possible low representativity of the replies to the questionnaires; however, the questionnaires were by their nature targeted to a specific niche of professionals, with a good coverage of the main stakeholders involved in the design and production of railway signalling systems.

We are also aware of the limits of the proposed questionnaires, which aimed mainly at a rapid collection of data, in the end providing only superficial data on the quite diverse background and experience of the respondents. No definition of formal methods, nor of formal (specification, development, verification) tools was given in advance to the respondents. While this allowed to probe the rather broad understanding of how formal methods are conceived in industry, at the same time it has reduced the importance of the results of the questionnaires by spreading the scores over a wide and variegated area of techniques and tools, which has required weakening the canonical definitions of formal methods and tools. The questionnaires also lacked a precise definition of terms that could easily be given different meanings by the respondents (e.g., "maturity", which could mean that the tool has been around for a while, appears polished, or is stable in the sense that it does not crash a lot).

Surely, more investigation is needed to refine the obtained results. An extended format for the questionnaires addressing the above limits should be prepared and proposed to a larger, more controlled, audience. Moreover, the latest conclusions drawn from the integration of the three questionnaires, regarding the most used tools and related expectations in terms of most relevant features and relevant quality aspects, have triggered our interest in understanding to what extent currently available tools, such as those cited in the questionnaires, actually satisfy the expectations: a specific investigation among professionals in this regard could form a solid base for subsequent research on the definition of readily available development processes that integrate formal and semi-formal tools, providing industry with clear paths to follow in different situations, with minimum friction and maximum benefit. The recent overview of the status of formal tools presented in [9] perfectly summarizes the current difficulties faced by users of such tools. However, the authors also propose a number of directions for improvement, both for the individual tool developer and for the academic community as a whole.

Acknowledgements This work has been partially funded by the ASTRail and the X2Rail-2 projects. These projects received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No. 777561 and No. 777465.

References

1. Ameur, Y.A., Boniol, F., Wiels, V.: Toward a wider use of formal methods for aerospace systems design and verification. International Journal on Software Tools for Technology Transfer **12**(1), 1–7 (2010)
2. Basile, D., ter Beek, M.H., Fantechi, A., Gnesi, S., Mazzanti, F., Piattino, A., Trentini, D., Ferrari, A.: On the Industrial Uptake of Formal Methods in the Railway Domain: A Survey with Stakeholders. In: IFM. LNCS, vol. 11023, pp. 20–29. Springer (2018)
3. Butler, M.J., Dghaym, D., Fischer, T., Hoang, T.S., Reichl, K., Snook, C.F., Tummeltshammer, P.: Formal Modelling Techniques for Efficient Development of Railway Control Products. In: RSSRail. LNCS, vol. 10598, pp. 71–86. Springer (2017)
4. Davis, J.A., Clark, M.A., Cofer, D.D., Fifarek, A., Hinchman, J., Hoffman, J.A., Hulbert, B.W., Miller, S.P., Wagner, L.G.: Study on the Barriers to the Industrial Adoption of Formal Methods. In: FMICS. LNCS, vol. 8187, pp. 63–77. Springer (2013)
5. 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)
6. Fantechi, A.: Twenty-Five Years of Formal Methods and Railways: What Next? In: SEFM. LNCS, vol. 8368, pp. 167–183. Springer (2013)
7. Fantechi, A., Ferrari, A., Gnesi, S.: Formal Methods and Safety Certification: Challenges in the Railways Domain. In: ISoLA. LNCS, vol. 9953, pp. 261–265. Springer (2016)
8. Ferrari, A., ter Beek, M.H., Mazzanti, F., Basile, D., Fantechi, A., Gnesi, S., Piattino, A., Trentini, D.: Survey on Formal Methods and Tools in Railways: The ASTRail Approach. In: RSSRail. LNCS, vol. 11495, pp. 226–241. Springer (2019)
9. Garavel, H., Mateescu, R.: Reflections on Bernhard Steffen's Physics of Software Tools. In: Models, Mindsets, Meta: The What, the How, and the Why Not? LNCS, vol. 11200, pp. 186–207. Springer (2019)
10. Nyberg, M., Gurov, D., Lidström, C., Rasmusson, A., Westman, J.: Formal Verification in Automotive Industry: Enablers and Obstacles. In: ISoLA. LNCS, vol. 11247, pp. 139–158. Springer (2018)
11. Plat, N., van Katwijk, J., Toetenel, H.: Application and benefits of formal methods in software development. Software Engineering Journal **7**(5), 335–346 (1992)
12. X2Rail-2 – Deliverable D5.1, Formal Methods (Taxonomy and Survey), Proposed Methods and Applications (16 May 2018), https://projects.shift2rail.org/download.aspx?id=b4cf6a3d-f1f2-4dd3-ae01-2bada34596b8