Formal methods for transport systems

Maurice H. ter Beek[1] · **Stefania Gnesi**[1] · **Alexander Knapp**[2]

Abstract
Formal methods and verification tools have been in use in the engineering of safety-critical transport systems for well over 30 years. In both the railway and the avionics domain, for instance, formal methods are specifically recommended in current international certification standards for ultra-dependable systems and for products at the highest integrity level. In fact, traditionally, the applications of formal methods and tools to such transport systems concern demonstrating, with the highest levels of assurance, the correct functioning of the software systems involved, such as train signalling systems to avoid collisions. More recently, however, formal methods and verification tools have started to be applied also to the scheduling and management of transport systems or networks, for instance to optimise the exploitation of a railway line or to improve the operational efficiency of a bus network. In this introduction to the special issue on "Formal Methods for Transport Systems", we outline some recent achievements for each of the above-mentioned types of application of formal methods and tools. These achievements are represented by three selected papers: one was selected from the "Formal Methods and Safety Certification: Challenges in the Railways Domain" track at the seventh *International Symposium On Leveraging Applications of Formal Methods, Verification and Validation* (ISoLA 2016); another one was selected from the 21st *International Workshop on Formal Methods for Industrial Critical Systems* and the 16th *International Workshop on Automated Verification of Critical Systems* (FMICS-AVoCS 2016); a final one was selected after an open call for contributions.

Keywords Formal methods · Formal verification · Model checking · Critical systems · Transport systems

1 Introduction

Many modern-day transport systems are supported by advanced software control systems. As for other industrial safety-critical systems, the correct functioning and overall safety guarantees of such software systems are of paramount importance. Therefore, the main causes of software failures—such as requirements defects, design faults and incorrect implementations—need to be excluded with the highest levels of assurance. To this aim, formal methods and verification tools have been in use in the engineering of safety-critical systems for well over 30 years [1–4]. In the railway and avionics domains, for instance, formal methods are specifically recommended for ultra-dependable systems and for products at the highest integrity level in current international certification standards [5,6].

Formal methods are specification languages for describing the behaviour of a system as a model with a precise semantics, thus allowing their associated formal verification tools to perform analyses over these system models [7]. Similar to other engineering disciplines, the envisioned advantage of the use of formal methods and tools is the expectation that appropriate mathematical modelling and analysis contributes to the correctness of the developed systems by eliminating flaws in the requirements or design during the initial development phases, i.e. before implementation. With respect to testing, a formal verification technique such as model checking moreover exhaustively verifies all possible behaviour—and it does so automatically, providing a counterexample in case a desired property is violated [8].

Traditionally, formal methods and verification tools are thus widely applied to transport systems in order to demonstrate, with the highest levels of assurance, the correct

✉ Maurice H. ter Beek
terbeek@isti.cnr.it; maurice.terbeek@isti.cnr.it

Stefania Gnesi
gnesi@isti.cnr.it

Alexander Knapp
knapp@informatik.uni-augsburg.de

[1] Istituto di Scienza e Tecnologie dell'Informazione, Consiglio Nazionale delle Ricerche, Pisa, Italy

[2] Institute for Software and Systems Engineering, Universität Augsburg, Augsburg, Germany

functioning of the software control systems involved (e.g. train signalling systems to avoid collisions).

Let us consider the railway sector, for instance. The European Union's Horizon 2020 framework programme for research and innovation has provided substantial financing of the Shift2Rail initiative.[1] Shift2Rail considers formal methods to be fundamental to the provision of safe and reliable technological advances to increase the competitiveness of the railway industry. In fact, a dedicated call was issued for analysing the suitability of formal methods to support the transition to the next generation of ERTMS/ETCS (European Rail Traffic Management System/European Train Control System) signalling systems, which will include satellite-based train positioning, moving block distancing and automatic driving. Several projects financed under this initiative respond to this call, amongst which the following three:

- ASTRail (SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block Validation) aims to introduce recent scientific results and methodologies as well as cutting-edge technologies from other transport domains, in particular avionics and automotive, in the railway domain. These novel applications and solutions must be carefully analysed in terms of safety and performance, leveraging on formal methods and tools. The project contains a work package on "Formal methods for the railway field".
- RUN2RAIL (Innovative RUNning gear soluTiOns for new dependable, sustainable, intelligent and comfortable RAIL vehicles) aims to propose solutions to improve future train equipment (e.g. making them more reliable, lighter, more comfortable and less noisy). This requires multidisciplinary research that combines the expertise of different branches of engineering (e.g. mechanical, materials, electronic and electrical) to elaborate models and formal methods for a set of advanced technological developments.
- X2Rail2 (Enhancing railway signalling systems based on train satellite positioning, on-board safe train integrity, formal methods approach and standard interfaces, enhancing Traffic Management System functions) aims to improve the performance of railway systems by introducing new functionalities, such as the application of GNSS (Global Navigation Satellite System) technology, which should revolutionise future signalling and automation systems. The project contains a work package on "Formal methods and standardisation for smart signalling systems".

More recently, formal methods and verification tools have started to be applied also to improve the scheduling and management of (smart) transport systems or networks, for instance to optimise the exploitation of a railway line or to improve the operational efficiency of a bus network (such as bus headway rebalancing or advanced bus arrival prediction systems).

Indeed, we are currently witnessing an interesting shift from the analysis of (embedded) software (systems) that *control* the correct/safe functioning of transport systems to software (systems) that *improve* the user experience and reliability of smart transport systems.

This special issue on "Formal Methods for Transport Systems" consists of three papers and this introduction; one was selected from the "Formal Methods and Safety Certification: Challenges in the Railways Domain" track at the seventh *International Symposium On Leveraging Applications of Formal Methods, Verification and Validation* (ISoLA 2016); another one was selected from the 21st *International Workshop on Formal Methods for Industrial Critical Systems* and the 16th *International Workshop on Automated Verification of Critical Systems* (FMICS-AVoCS 2016); the last paper resulted from an open call for papers.

The track "Formal Methods and Safety Certification: Challenges in the Railways Domain" [9], which took place on 11 October 2016, as part of the seventh *International Symposium On Leveraging Applications of Formal Methods, Verification and Validation* (ISoLA 2016) in Corfu, Greece, called for the research community to find effectively and conveniently implementable ways to develop:

- Suitable domain-specific modelling and analysis techniques, able to scale up to the ever-increasing complexity of railway systems.
- Alignment of (the usability of) verification techniques to industrial development processes and to the current certification guidelines.
- Formal and automated verification of large station interlockings, with the aim of decreasing certification costs.
- Cost reduction in verification of specific railway applications with respect to generic verification techniques.
- Standardisation of protocols and procedures, based on unambiguous definitions, in order to support the interoperability of different systems.

The proceedings appeared in Springer's Lecture Notes in Computer Science [10].

The 21st *International Workshop on Formal Methods for Industrial Critical Systems* and the 16th *International Workshop on Automated Verification of Critical Systems* (FMICS-AVoCS 2016), which were organised as a joint event from 26 September to 28 September 2016, in Pisa, Italy, called for contributions on the following, amongst others, topics of interest:

[1] www.shift2rail.org.

– Design, specification, refinement, code generation and testing of critical systems based on formal methods.
– Methods, techniques and tools to support the automated analysis, certification, debugging, learning, optimisation and transformation of critical systems, in particular distributed, real-time systems and embedded systems.
– Automated verification (e.g. model checking, theorem proving, SAT/SMT constraint solving, abstract interpretation, etc.) of critical systems.
– Verification and validation methods addressing shortcomings of existing methods with respect to their industrial applicability (e.g. scalability and usability issues).
– Case studies and experience reports on industrial applications of formal methods, focussing on lessons learnt or on the identification of new research directions.
– Impact of the adoption of formal methods on the development process and associated costs.
– Application of formal methods in standardisation and industrial forums.

The proceedings appeared in Springer's Lecture Notes in Computer Science [11].

Finally, an open call for papers dedicated to "Formal Methods and Automated Verification of Critical Systems", which welcomed research papers containing novel, previously unpublished results in all areas related to the topics of the FMICS and AVoCS workshop series, was issued in November 2016. A total of 14 papers were submitted. Based upon a thorough reviewing process, the editors decided to accept nine papers; six of them will appear in the special issue FMICS-AVoCS of the Springer journal *Software Tools for Technology Transfer* (STTT), while three papers are included in this special issue, due to their focus on transport systems.

The selected papers in this special issue cover three application domains, ranging from railway system signalling to public transport network operation. One of the papers focuses on the traditional use of formal methods and verification tools for modelling and verifying correctness and safety issues of transport systems, while the other two papers address the relatively novel use of formal methods and tools for improving the scheduling and management of transport systems.

Outline of this introduction Our discussion of the papers selected for this special issue is organised as follows. Section 2 discusses modelling and simulating a complete Thai railway signalling system with Coloured Petri Nets covering a total of nine fundamental safety properties. Section 3 discusses experiences with modelling and verifying deadlock avoidance in train scheduling using a total of seven different formal methods and associated tools. Section 4 discusses the use of spatial and spatio-temporal model checking to analyse the operational efficiency of bus networks. Section 5 concludes this introduction.

2 Formally specifying and simulating complete models to validate transport control systems

Formal methods and tools have been applied to railway signalling systems and interlockings for quite some time. In particular, fully automated verification techniques, such as model checking, have proved to be an indispensable tool for understanding and validating the properties of these large, safety-critical and error-prone systems. Whereas many approaches concentrate on specific properties, like route interlocking for preventing train collisions, the first paper of this special issue, *Modelling and simulating a Thai railway signalling system using Coloured Petri Nets* by Vanit-Anunchai [12], strives to develop a comprehensive model for the State Railway of Thailand (SRT).

Starting from interlocking tables, a Coloured Petri Net (CPN) model is presented that has proven to be appropriate for the necessary communication with SRT's signal engineers. The main motivation for giving such a complete model is that premature abstraction (leading to an incomplete model) could result in error masking between different desirable properties of an interlocking. Nine such properties, like route interlocking, flank protection or route normalisation, are identified and integrated into the model. Despite its comprehensiveness, some properties, like route interlocking and flank protection, still can be verified automatically by state space exploration. For other properties, simulation supported by visualisation is offered as a complementary exploration technique.

Indeed, if an error is found in an abstract, though incomplete model and it can be simulated in the concrete system, abstraction has worked well. But if no error can be detected, a more concrete and complete model has to be taken into account. For problems of the size of railway interlockings, soon a point will be reached where such a more comprehensive model can no longer be analysed automatically.

Vanit-Anunchai considers the position that partial validation of a complete model is sometimes to be preferred over fully automated validation of an incomplete model. The modelling effort itself is still very worthwhile, because it gives insights in the intricacies of the particular engineering domain and it fosters communication and discussion with the engineers. Ideally, tractable parts of the comprehensive model can be derived automatically. On the other hand, simulation and testing remain possible techniques for analysing the comprehensive model.

3 Increasing confidence in verifying transport systems by applying formal methods diversity

A typical scheduling problem in the railway domain concerns the dispatching of trains without causing deadlocks due to a train's route being blocked by another train. The second paper of this special issue, *Towards Formal Methods Diversity in Railways: an Experience Report with Seven Frameworks* by Mazzanti et al. [13], reports on the authors' experience with the modelling and analysis of seven models of a deadlock avoidance algorithm in even so many formal verification environments.

The specific algorithm was previously implemented by the authors (cf., for example, [14]) as part of the Automatic Train Supervision (ATS) system of a Communications-Based Train Control (CBTC) system [15]. CBTC systems are mainly used to control driverless metro and suburban trains. The railway layout considered consists of eight trains and two critical sections, resulting in a logical design with a non-trivial state space of 1,636,535 configurations. The seven verification environments considered in the paper are UMC, Promela/SPIN, NuSMV, mCRL2, CSP/FDR4, Coloured Petri Nets/CPN Tools and CADP (cf. the paper for references).

None of these formal verification frameworks has been certified according to the CENELEC EN 50128 standard for the development of safety-critical software in the railway sector, which recommends the use of formal methods during the design and implementation of railway applications. Mazzanti et al. advocate to adopt the concept of *formal methods diversity* in the railway sector, inspired by code/design diversity (cf., for example, [16]) and based on the hypothesis that the application of diverse, non-certified formal verification tools on a replication of the same design may increase confidence in the correctness of the verification results.

4 Spatio-temporal model checking to analyse operational correctness of transport systems

In modern (smart) public transport systems, it is becoming more and more important to guarantee not only safety properties, but also data correctness as well as operational correctness. The satisfactory, well-regulated operation of such transport systems depends on accurate fleet management, which is often based on automatic vehicle location (AVL) systems. The correctness of AVL data, which constitutes crucial input data for vehicle arrival prediction systems, thus directly influences the latter systems' operational correctness, which is an important measure of service quality. The third and final paper of this special issue, *Spatio-temporal model checking of vehicular movement in public transport systems* by Ciancia et al. [17], reports on applying both purely spatial and combined spatio-temporal model-checking techniques to assess the data as well as operational correctness of a bus network.

To set the stage, Ciancia et al. produce a digital image of the GPS data received from Lothian buses in the city of Edinburgh. They use spatial model checking to answer questions related to both data correctness (like "Is this bus really so far off-route?") and operational correctness (like "Is this bus catching up with the one in front?") by considering different *views* of the data. A "satellite view" of all buses at one moment in time is used to deal with issues concerning congestion and adjacency, while a "passenger view"of one bus at all moments in time is used for issues concerning journeys and routes.

Spatio-temporal model checking, on the other hand, is used to analyse the so-called headway of buses, which is a measure of the distance or time between vehicles in a transport system. This metric is fundamental to determine the risk of *clumping*, which is known to be one of the most frequent causes of user dissatisfaction in frequent bus services. Clumping occurs when two or more buses running the same route get too close to each other, generally due to a bus running late finding more and more people waiting at the bus stops, resulting in further delay and later buses finding less and less people at the bus stops, thus catching up with the bus in front. Finally, also the effect of headway rebalancing policies is analysed and validated by means of spatio-temporal model checking.

Hence, Ciancia et al. consider spatial and spatio-temporal model checking to be suitable means for the verification of both data and operational correctness, such as vehicle monitoring (positioning) and scheduling efficiency in (smart) transport networks.

5 Conclusion

We have discussed the long-standing tradition of the use of formal methods and automated verification tools for the specification and functional correctness analysis of software systems in safety-critical domains such as railways, automative and avionics, recorded in numerous standards in the fields, as well as the recent shift towards the use of formal methods and novel verification techniques for the scheduling and management of (smart) transport systems or networks.

We presented the three selected papers constituting this special issue, discussing the following topics. First, for problems the size of railway interlockings, partial validation of a complete model is sometimes to be preferred over fully automated validation of an incomplete model, due to the risk of premature abstractions causing error masking of desirable

properties. In the absence of full validation, the modelling effort may still be worth the while because it highlights the intricacies of the particular engineering domain and fosters communication and discussion with the engineers involved. Secondly, the possible adoption of the concept of formal methods diversity in the railway sector, based on the assumption that the application of diverse, non-certified formal verification tools on a replication of the same specification may increase confidence in the correctness of the verification results. Lastly, the verification of data correctness and operational correctness with spatial and spatio-temporal model-checking techniques improve vehicle monitoring and the efficiency of scheduling policies in smart transport networks.

Acknowledgements We would like to thank all authors for their contributions and the reviewers of ISoLA 2016, FMICS-AVoCS 2016 and in particular those of this special issue for their reviews.

References

1. 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)
2. Gigante, G., Pascarella, D.: Formal methods in avionic software certification: the DO-178C perspective. In: Margaria, T., Steffen, B. (eds.) Proceedings of the 5th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Applications and Case Studies (ISoLA 2012), Part II. Lecture Notes in Computer Science, vol. 7610, pp. 205–215. Springer (2012)
3. 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. Lecture Notes in Computer Science, vol. 8368, pp. 167–183. Springer (2013)
4. Gnesi, S., Margaria, T.: Formal Methods for Industrial Critical Systems: A Survey of Applications. Wiley, Hoboken (2013)
5. European Committee for Electrotechnical Standardization: CENELEC—EN 50128: railway applications—communication, signalling and processing systems—software for railway control and protection systems, June (2011). http://standards.globalspec.com/std/1678027/cenelec-en-50128
6. Radio Technical Commission for Aeronautics: RTCA DO–178: software considerations in airborne systems and equipment certification, December (2011). http://standards.globalspec.com/std/1830812/rtca-do-178
7. Almeida, J.B., Frade, M.J., Pinto, J.S., de Sousa, S.M.: An overview of formal methods tools and techniques. In: Rigorous Software Development: An Introduction to Program Verification, pp. 15–44. Springer (2011)
8. Baier, C., Katoen, J.-P.: Principles of Model Checking. MIT Press, Cambridge (2008)
9. Fantechi, A., Ferrari, A., Gnesi, S.: Formal methods and safety certification: challenges in the railways domain. In: Margaria, Steffen (eds.) [10], pp. 261–265
10. 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), Part II. Lecture Notes in Computer Science, vol. 9953. Springer (2016)
11. ter Beek, M.H., Gnesi, S., Knapp, A. (eds.): Critical Systems: Formal Methods and Automated Verification—Proceedings of the Joint 21st International Workshop on Formal Methods for Industrial Critical Systems and 16th International Workshop on Automated Verification of Critical Systems (FMICS-AVoCS 2016). Lecture Notes in Computer Science, vol. 9933. Springer (2016)
12. Vanit-Anunchai, S.: Modelling and simulating a Thai railway signalling system using Coloured Petri Nets. Int. J. Softw. Tools Technol. Transf. (2018). https://doi.org/10.1007/s10009-018-0482-9
13. 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. (2018). https://doi.org/10.1007/s10009-018-0488-3
14. Mazzanti, F., Spagnolo, G.O., Ferrari, A.: Designing a deadlock-free train scheduler: a model checking approach. In: Badger, J.M., Rozier, K.Y. (eds.) Proceedings of the 6th International NASA Formal Methods Symposium (NFM 2014). Lecture Notes in Computer Science, vol. 8430, pp. 264–269. Springer (2014)
15. IEEE Vehicular Technology Society: IEEE Std 1474.1-2004(R2009): IEEE standard for communications-based train control (CBTC) performance and functional requirements, February (2005). https://doi.org/10.1109/IEEESTD.2004.95746
16. Littlewood, B., Popov, P., Strigini, L.: Modeling software design diversity: a review. ACM Comput. Surv. **33**(2), 177–208 (2001)
17. Ciancia, V., Gilmore, S., Grilletti, G., Latella, D., Loreti, M., Massink, M.: Spatio-temporal model checking of vehicular movement in public transport systems. Int. J. Softw. Tools Technol. Transf. (2018). https://doi.org/10.1007/s10009-018-0483-8