Formal Methods and Safety Certification: Challenges in the Railways Domain

Alessandro Fantechi[1,2,3(✉)], Alessio Ferrari[2], and Stefania Gnesi[2]

[1] DINFO, Università degli Studi di Firenze, Via S. Marta 3, Florence, Italy
fantechi@dsi.unifi.it
[2] Istituto di Scienza e Tecnologie dell'Informazione
"A. Faedo" CNR, Via Moruzzi 1, Pisa, Italy
{alessio.ferrari,stefania.gnesi}@isti.cnr.it
[3] DTU Compute, Technical University of Denmark, Kongens Lyngby, Denmark

1 Motivation

The railway signalling sector has historically been a source of success stories about the adoption of formal methods in the certification of software safety of computer-based control equipment. Although it is not possible to exhaustively cite such stories here, we can refer to some witnesses in the two main classes in which we can roughly divide railway signalling systems:

– *ATP/ATC (Automatic Train Protection/Control)* systems guarantee safe speed and braking control for trains, along the line, where the main safety criterion is to guarantee that two trains travelling at speed in the same direction stay a safe distance apart. The basic concept in ATP/ATC is the *braking curve*: safety is guaranteed if the speed is always below the line of the braking curve; should the speed go above the line, emergency braking is enforced.
These systems accommodate both train distancing and protection of singular points of the line: for the first purpose a line is divided in sections of which appropriate sensors detect occupancy by a train. Distancing is obtained by ensuring that at any moment the speed of the train is such that the train can be brought to a halt before entering in an occupied section, that is, the braking curve is at zero at the entrance of the occupied section: the value of allowed speed given by the braking curve depend on the number of free sections in front of the train. Protection of singular points of the line (e.g., an open level crossing) is obtained by setting the braking curve at zero at the protected point.
ATP/ATC systems are constituted by on-board components that receive information from wayside components. In the early computer-based systems of this kind, this communication is rather simple and occurs at specific points of the line. As a consequence, the safety enforcing algorithms were not excessively complex and were directly amenable to formal specification [4].
– *Interlocking* systems establish safe routes through the intricate layout of tracks and points. Interlocking systems have since many years called for a direct application of model checking, due to the fact that their safety properties can

T. Margaria and B. Steffen (Eds.): ISoLA 2016, Part II, LNCS 9953, pp. 261–265, 2016.
DOI: 10.1007/978-3-319-47169-3_18

be expressed in temporal logic, and that their specifications by means of control tables can be directly formalized [3,11,13,14]. Typical of these verification tasks is the combinatorial state space explosion problem, due to the high number of boolean variables involved: the first applications of model checking have therefore addressed portions of an interlocking system (e.g., [2,8]); but even recent works [7,15,18] show that routine verification of interlocking designs for large stations is still a challenge for model checkers.

The latest technological evolutions of signalling systems promise a significant improvement on transport capacity, on the regularity of the service, on the very quality and safety of the offered service. These solutions are increasingly based on the presence, on board trains and at ground, of processors that deal with more and more complex real-time information, and on the adoption of wireless communication links between trains and ground.

Examples of this trend are the roll-out of ERTMS/ETCS (European Rail Traffic Management System/European Train Control System) to improve capacity and enhance cross-border operation within Europe, and the CBTC (Communication Based Train Control) systems deployed in metro and suburban railways to improve capacity and to add automated driving capabilities.

This evolution poses big challenges to the consolidated safety certification processes, and raises concerns about the guarantees to maintain the typically high standards of safety in railway operation whilst being able to satisfy availability, capacity and interoperability requirements. The actual achievement of capacity, availability and interoperability improvements prospected for the future is still a challenge, also in view of the necessary economic investment that these new technologies require. In addition, given the heavy presence of wireless communication links in novel railway systems, security has become a central issue to cope with. Finally, railway systems are by nature *green* transportation systems, which have to keep this desirable attribute even in presence of increasing capacity requirements. Hence, energy consumption is also a primary aspect to consider.

New visionary systems are also beginning to be proposed within the railway signalling community [5]. These have in common the removal of historic assumptions and constraints that have ruled railway safety so far, by resorting to the possibilities offered by technological advances. In particular, moving and distributing the intelligence, that is so far concentrated in a few control centres, is seen as a step towards more efficient, less expensive, more easily maintainable control and management systems. Although distribution makes safety certification much more complex, it promises a more flexible operation and reconfiguration to address planned and emergency changes. These ideas will be the basis for future innovative system architectures. Analysing their safety will be vital to ensure that such innovations will be fit for purpose.

Coping with the challenges posed by the increasing scale and complexity of railway systems, and by the novel technologies available, require the formal methods community to extend and customise the modelling and verification methodologies that showed their effectiveness in earlier computer-based railway systems.

In particular, the community is asked to provide formal solutions that: (a) can deal with *systems-of-systems* that, besides interoperability, have to guarantee high safety and capacity standards; (b) are able to enforce system dependability aspects that go beyond safety – especially security and availability; (c) take into account the *cyber-physical*, hybrid, nature of railway systems to cope, e.g., with the issue of energy consumption.

Addressing these challenges requires an effort from the formal methods research community as well as a stronger cross-fertilisation with railway systems developers, operators, and certification authorities. On the one hand, this will enable the research community to have a proper in-depth understanding of the railway domain, and to focus on solutions to real-world needs of the domain. On the other hand, this will ensure that solutions proposed within the academic world will be properly tailored to be usable, and acceptable, for practitioners.

2 Goals and Contributions

Inspired by the track on "Formal Methods for Intelligent Transportation Systems" held at ISOLA 2012 [6], which actually focused mostly on railway applications, the track "Formal Methods and Safety Certification: Challenges in the Railways Domain" of this year edition aims to present some advanced results addressing the challenges discussed above, in order to show how existing modelling techniques are extended and customized to cope with such challenges. Although addressing different aspects of the domain, the contributions to the track share the approach of basing their specific analysis of different dependability characteristic on a rigorous formal modelling approach.

Three contributions to this track concentrate on the big challenge of verifying large railway interlocking systems, proposing different verification strategies to attack their complexity, in order to decrease the cost of their safety certification. While [10] proposes the adoption of static analysis for the early detection of defects in the specification of the interlocking logics, [12] exploits a compositional approach for attacking large systems of this class. The short contribution [17] describes an open integrated toolset for interlocking verification. The interest of the research community to this challenge is witnessed also by a contribution to the track on "Variability Modelling for Scalable Software Evolution" [9], which proposes an incremental approach based on techniques from the Software Product Lines discipline in order to reduce the time and cost for certification at system updates and layout changes of an interlocking system.

Not only safety contributes to the dependability of nowadays signalling systems: in the railway domain, safety is typically obtained at the cost of reducing service, by halting trains in case of adverse situations; in the current quest of gaining more and more capacity from existing rail lines, availability is indeed of paramount importance. Contribution [16] shows how modelling and model checking techniques used for safety verification can be employed as well, although at a different abstraction level, to establish liveness of a railway line by the detection of possible deadlocks.

Contribution [1] shows how formal modelling can be exploited as well for analysing particular aspects of physical components of the railway system: a precise analysis of energy consumption of switch heaters, although a very localized and apparently minor issue, contributes to the overall safety and availability assessment of a railway system in an important way. In addition, the contribution shows how formal techniques can be used to deal with cyber-physical aspects related to energy consumption.

It is our opinion that, notwithstanding the limited space available, the contributions to the track succeed to give a glance of the state of the art and of the opportunities offered by up-to-date formal modelling and verification techniques and tools in the railway domain. In the future, we foresee a stronger effort towards refining the proposed solutions, and towards a major focus on the issues related to *security*, and to the interplay between security and the other dependability attributes.

References

1. Basile, D., Di Giandomenico, F., Gnesi, S.: Tuning energy consumption strategies in the railway domain: a model-based approach. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016, Part II. LNCS, vol. 9953, pp. 315–330. Springer, Heidelberg (2016)
2. Bernardeschi, C., Fantechi, A., Gnesi, S., Larosa, S., Mongardi, G., Romano, D.: A formal verification environment for railway signaling system design. Formal Methods Syst. Des. **12**(2), 139–161 (1998)
3. Bonacchi, A., Fantechi, A., Bacherini, S., Tempestini, M., Cipriani, L.: Validation of railway interlocking systems by formal verification, a case study. In: Counsell, S., Núñez, M. (eds.) SEFM 2013. LNCS, vol. 8368, pp. 237–252. Springer, Heidelberg (2014). doi:10.1007/978-3-319-05032-4_18
4. Da Silva, C., Dehbonei, B., Mejia, F.: Formal specification in the development of industrial applications: subway speed control system. In: Proceedings 5th IFIP Conference on Formal Description Techniques for Distributed Systems and Communication Protocols (FORTE 1992), Perros-Guirec, pp. 199–213. North-Holland (1993)
5. Fantechi, A.: Formal techniques for a data-driven certification of advanced railway signalling systems. In: ter Beek, M.H., Gnesi, S., Knapp, A. (eds.) FMICS-AVoCS 2016. LNCS, vol. 9933, pp. 231–245. Springer, Heidelberg (2016). doi:10.1007/978-3-319-45943-1_16
6. Fantechi, A., Flammini, F., Gnesi, S.: Formal methods for intelligent transportation systems. In: Margaria, T., Steffen, B. (eds.) ISoLA 2012. LNCS, vol. 7610, pp. 187–189. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34032-1_19
7. Ferrari, A., Magnani, G., Grasso, D., Fantechi, A.: Model checking interlocking control tables. In: Schnieder, E., Tarnai, G. (eds.) FORMS/FORMAT 2010, pp. 107–115. Springer, Heidelbreg (2010). doi:10.1007/978-3-642-14261-1_11
8. Groote, J.F., van Vlijmen, S., Koorn, J.: The safety guaranteeing system at station Hoorn-Kersenboogerd. In: Logic Group Preprint Series 121. Utrecht University (1995)
9. Hähnle, R., Muschevici, R.: Towards incremental validation of railway systems. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016, Part II. LNCS, vol. 9953, pp. 433–446. Springer, Heidelberg (2016)

10. Haxthausen, A.E., Østergaard, P.H.: On the use of static checking in the verification of interlocking systems. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016, Part II. LNCS, vol. 9953, pp. 266–278. Springer, Heidelberg (2016)
11. Haxthausen, A.E., Peleska, J., Pinger, R.: Applied bounded model checking for interlocking system designs. In: Counsell, S., Núñez, M. (eds.) SEFM 2013. LNCS, vol. 8368, pp. 205–220. Springer, Heidelberg (2014). doi:10.1007/978-3-319-05032-4_16
12. Macedo, H.D., Fantechi, A., Haxthausen, A.E.: Compositional verification of multi-station interlocking systems. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016, Part II. LNCS, vol. 9953, pp. 279–293. Springer, Heidelberg (2016)
13. James, P., Lawrence, A., Moller, F., Roggenbach, M., Seisenberger, M., Setzer, A., Kanso, K., Chadwick, S.: Verification of solid state interlocking programs. In: Counsell, S., Núñez, M. (eds.) SEFM 2013. LNCS, vol. 8368, pp. 253–268. Springer, Heidelberg (2014). doi:10.1007/978-3-319-05032-4_19
14. James, P., Moller, F., Nguyen, H.N., Roggenbach, M., Schneider, S., Treharne, H., Trumble, M., Williams, D.: Verification of scheme plans using CSP||B. In: Counsell, S., Núñez, M. (eds.) SEFM 2013. LNCS, vol. 8368, pp. 189–204. Springer, Heidelberg (2014). doi:10.1007/978-3-319-05032-4_15
15. Limbrée, C., Cappart, Q., Pecheur, C., Tonetta, S.: Verification of railway interlocking - compositional approach with OCRA. In: Lecomte, T., Pinger, R., Romanovsky, A. (eds.) RSSRail 2016. LNCS, vol. 9707, pp. 134–149. Springer, Heidelberg (2016). doi:10.1007/978-3-319-33951-1_10
16. Mazzanti, F., Ferrari, A., Spagnolo, G.O.: Experiments in formal modelling of a deadlock avoidance algorithm for a CBTC system. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016, Part II. LNCS, vol. 9953, pp. 297–314. Springer, Heidelberg (2016)
17. Nguyen, H.N., Roggenbach, M., Wang, X., Treharne, H.: The railway verification toolset OnTrack. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016, Part II. LNCS, vol. 9953, pp. 294–296. Springer, Heidelberg (2016)
18. Vu, L.H., Haxthausen, A.E., Peleska, J.: Formal modeling and verification of interlocking systems featuring sequential release. In: Artho, C., Ölveczky, P.C. (eds.) FTSCS 2014. CCIS, vol. 476, pp. 223–238. Springer, Heidelberg (2015). doi:10.1007/978-3-319-17581-2_15