Formal methods for Distributed Computing in future Railway systems

Alessandro Fantechi[1,2], Stefania Gnesi[2], and Anne Haxthausen[3]

[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, Pisa, Italy
Via Moruzzi 1, Pisa, Italy
alessio.ferrari@isti.cnr.it, stefania.gnesi@isti.cnr.it
[3] DTU Compute, Technical University of Denmark

1 Motivation

The growingly wide deployment of ERTMS-ETCS systems on high speed lines as well as on freight corridors is already a witness to the possible achievement of high safety standards by means of distributed control algorithms, that span over geographical areas and are able to safely control large physical systems. In ERTMS-ETCS the guarantee of global properties (such as safety) emerges from the conformance of the subsystems to well-established communication protocols and standards.

Formal methods are already one of the technologies used within railway industries, and the Shift2Rail program insists on the synergy of formal methods and standardised interfaces for a seamless connection of independent (formally specified) equipments and devices through well-defined interfaces, a synergy that can guarantee global dependability properties.

Most of the crucial decisions needed to guarantee safety are still taken at centralized places (such as the Radio Block Centre RBC), and the topology of such systems can be considered as a two layers network, the lower layer being just a connection of mobile systems with a centralized unit (the RBC), while the higher layer connects through a fixed network the RBCs with each other and the traffic management systems.

Following an increasingly popular trend for Cyber-Physical Systems, a more dynamic network connection among mobile components can be envisaged, in which decisions are actually taken in a distributed fashion. An example is given by proposals of fully distributed interlocking systems, where the route reservation is a global concept to be negotiated between the nodes [?,?,?]. Another example is the virtual coupling concept, in which the strict cross-control between coupled trains has to be negotiated locally, while the global behavior of the set of coupled trains has to follow the rules dictated by the ETCS control system [?,?].

Pros and Cons of distributing vital decisions is a matter of active research, especially considering that the increasing importance of communication raises the need of uncertainty being taken into account in a railway control system: is the same safety level achievable by distributed decisions w.r.t. centralised ones? How formal methods can guarantee safety in such context?

2 Goals

The adoption of formal methods in railway signalling has been already the subject of two tracks of past ISOLA conferences. The track on "Formal Methods for Intelligent Transportation Systems" held at ISOLA 2012 [?], was actually focused mostly on railway applications, and this was indeed a recognition on how much already the railway signalling sector had been a source of success stories about the adoption of formal methods. The more railway-focused track "Formal Methods and Safety Certification: Challenges in the Railways Domain" held at ISOLA 2016 [?] aimed at presenting advanced results and at addressing the challenges posed by the increasing scale and complexity of railway systems.

In 2019, a specific workshop colocated with the DisCoTec federated conference on distributed computing, DisCoRail 2019, was set up with the aim of discussing how distributed computing was affecting the railway signalling domain. It has soon appeared evident that the high expectations on safety, but also on availability and performance of future railway signalling systems, in presence of a high degree of distribution, could be addressed only by a systematic adoption of formal methods in their definition and development. For this reason DisCoRail has joined ISOLA, and inherits at this regard some traits of the two mentioned past tracks.

Hence the aim of this track is to discuss (1) how distributed computing can change, and is actually changing, the domain of railway signaling and train control systems, and (2) how formal methods can help to address challenges arising from this change.

3 Contributions

Two contributions [?,?] discuss two different frameworks in which an established formal method in the railway domain, B, is extended to deal with distributed applications in an industrial setting.

Two other contributions of this track focus on formal verification by model checking of distributed interlocking systems [?,?], considering different modelling and verification strategies, and evaluating the scalability of formal verification, typically affected by state explosion problems when dealing with systems dealing with large station and network layouts.

The paper [?] presents a completely different view on how distributed computing can be exploited to achieve better performance/cost ratio of signalling equipment, that is, moving to the cloud the (safety-related) data that constitute the digital twin of the physical plants: the problems raised by this revolutionary proposal are discussed in detail.

Given the importance recognized by the Shift2Rail program to the very topics of this track, a session dedicated to presentations of running Shift2Rail projects contributes to the track program. The session includes paper [**?**] on the 4SECURail project, aimed at providing a demonstrator of state-of-the-art formal methods and tools, applied on a railway signalling subsystem described by means of standard interfaces, and a brief account of the RAILS project [**?**], aimed at investigating the potential of AI in the rail sector in continuity with ongoing research in railways, The session is completed by a brief account of a parallel running project, FORMASIG [**?**] aimed as well at formal definition of standardized interfaces. Further to the contributions presented in this volume the actual discussion at the conference is expected to include interventions coming from other Shift2Rail projects.

It is our opinion that, notwithstanding the limited space available, the contributions to the track sucfceed to give a glance of the state of the art and of the opportunities of the application of formal techniques to the distributed systems of systems represented by the future railway signalling systems.

References

1. Basile, D., ter Beek, M.H., Fantechi, A., Ferrari, A., Gnesi, S., Masullo, L., Mazzanti, F., Piattino, A., Trentini, D.: Designing a Demonstrator of Formal Methods for Railways Infrastructure Managers. In this volume.
2. Collart-Dutilleul, S., Bon, P.: A modular design framework to assess intelligent trains. In this volume.
3. Fantechi, A., Flammini, F., Gnesi, S.: Formal Methods for Intelligent Transportation Systems. 5th International Symposium, ISoLA 2012, vol.2, Lecture Notes in Computer Science, vol. 1 7610, pp. 187-189, Springer (2012). 10.1007/978-3-642-34032-1_19
4. Fantechi, A., Ferrari, A., Gnesi, S.: Formal Methods and Safety Certification: Challenges in the Railways Domain, ISoLA 2016 vol.2, Lecture Notes in Computer Science vol. 9953, pp. 261–265, Springer (2016). 10.1007/978-3-319-47169-3_18
5. Fantechi, A., Gnesi, S., Haxthausen, A., van de Pol, J., Roveri, M., Treharne, H.: SaRDIn - A safe reconfigurable distributed interlocking. In: Proc. 11th World Congress on Railway Research, WCRR. Ferrovie dello Stato Italiane, Milano (2016)
6. Fantechi, A., Haxthausen, A.E.: Safety interlocking as a distributed mutual exclusion problem. In: Howar, F., Barnat, J. (eds.) Formal Methods for Industrial Critical Systems - 23rd International Conference, FMICS 2018, Maynooth, Ireland, September 3-4, 2018, Proceedings. Lecture Notes in Computer Science, vol. 11119, pp. 52–66. Springer (2018). 10.1007/978-3-030-00244-2_4
7. Geisler, S., Haxthausen, A.E.: Model Checking a Distributed Interlocking System Using k-induction with RT-Tester. In this volume.
8. Flammini, F., Vittorini, V.: RAILS: Roadmaps for AI integration in the raiL Sector. In this volume.
9. Flammini, F., Marrone, S., Nardone, R., Petrillo, A., Santini, S., Vittorini, V.: Towards railway virtual coupling. In: International Transportation Electrification Conference (ITEC). IEEE, Nottingham, UK (2018). 10.1109/ESARS-ITEC.2018.8607523
10. Haxthausen, A.E. Peleska, J.: Formal development and verification of a distributed railway control system. IEEE Trans. Software Eng. **26**(8), 687–701 (2000). 10.1109/32.879808

11. Laursen, P.L., Trinh, V.A.T., Haxthausen, A.E. Formal Modelling and Verification of a Distributed Railway Interlocking System Using UPPAAL. In this volume.
12. Lecomte, T., Comptier M., Molinero, J., Sabatier, D.: Ensuring Safety with System Level Formal Modelling. In this volume.
13. Bouwman, M., Luttik, B., Rensink, A., Stoelinga, M., van der Wal, D.: Formal Methods in Railway Signalling Infrastructure Standardisation Processes. In this volume.
14. Peleska, J.: New Distribution Paradigms for Railway Interlocking. In this volume.
15. UIC: Virtually coupled trains, `http://www.railway-energy.org/static/Virtually_coupled_trains_86.php`. Accessed 12 Aug. 2020.