Formal Methods for Distributed Control Systems of Future Railways

Fantechi, Alessandro; Gnesi, Stefania; Haxthausen, Anne E.

Published in:
Leveraging Applications of Formal Methods, Verification and Validation

Link to article, DOI:
10.1007/978-3-031-19762-8_19

Publication date:
2022

Document Version
Peer reviewed version

Formal Methods for Distributed Control Systems of Future Railways

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

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

1 Motivations and Goals

The adoption of formal methods in railway signalling has been the subject of specific tracks of past ISOLA conferences since a decade. The track on "Formal Methods for Intelligent Transportation Systems" held at ISOLA 2012 [3] was actually focused on railway applications, as a recognition on how much already the railway signalling sector had been a source of success stories about the adoption of formal methods. The "Formal Methods and Safety Certification: Challenges in the Railways Domain" track of ISOLA 2016 [2] was aimed at discussing advanced results and addressing the challenges posed by the increasing scale and complexity of railway systems. In 2019, a workshop colocated with the DisCoTec federated conference on distributed computing, DisCoRail ("Formal methods for DIStributed COmputing in future RAILway system") 2019, was set up with the aim of discussing how distributed computing was affecting the railway signalling domain, given that the new technologies being applied in this domain (with a main example represented by the wide deployment of ERTMS-ETCS systems on high speed lines as well as on freight corridors) were transforming railways in a very large geographic distributed computing system. 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. This view has been shared by several projects within the Shift2Rail Joint Undertaking, that were also represented in the following edition of the DisCoRail workshop, that joined ISOLA in 2020/21 [4] (track on "Formal methods for DIStributed COmputing in future RAILway systems").

The DisCoRail 2019 workshop and the ISOLA DisCoRail track of 2021 have therefore discussed the intertwining of formal methods and distributed computing in the design and development of innovative train control systems, two dimensions naturally stemming from the two fundamental characteristics of this class of systems, namely that their functions are intrinsically distributed between

trains and wayside equipments, and that such functions are safety-critical, calling for rigorous proof of their safety.

Distribution of functionality enables distributing decisions as well. Currently, most of the crucial decisions needed to guarantee safety are however taken at centralised locations (such as the Radio Block Centre – RBC – in ETCS). Whether distributing vital decisions is indeed a matter of active research, especially considering that the related increasing importance of communication raises the need of uncertainty being taken into account: is the same safety level achievable by distributed decisions w.r.t. centralised ones? How formal methods can guarantee safety in such context? What about availability, interoperability, cybersecurity?

Moreover, the current research on autonomous driving for cars is inspiring a vision of autonomous trains in the next future. Autonomy requires even more distributed decisions based on local knowledge of the surrounding environment acquired also through AI-enabled sensors, e.g. employing artificial vision. Can formal methods be exploited to provide the necessary safety assurance for these systems?

Following the success of the previous DisCoRail editions, the track aims for a fruitful discussion on these topics between researchers and experts from industry and academia that have addressed these aspects in research and development projects.

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.

2 Contributions

The first three contributions analyse under different points of view the challenges posed by distribution and autonomy. The contribution [7] introduces those posed by advanced signalling systems in which AI will be a main enabling technology, discussing how formal methods research can address such challenges and outlining research problems that need to be further developed.

The paper [5] focuses on the effects that uncertainty on critical parameters (such as position or speed) can have on dependability of railway signalling systems, surveying various studies that have used state-based formal modelling of the system behaviour for a quantitative evaluation of such effects.

Certification of autonomous train operation systems using AI-based technology is discussed by [8], that considers existing standards and required modifications or extensions of existing standards.

The next two papers present instead specific solutions, also based on formal methods, to specific issues of future railway systems. Software Defined Networking (SDN) is proposed by [1] as a paradigm useful to dynamically reconfigure the network for an effective management of communication flows produced by moving trains. The paradigm is supported by a methodological framework based on model-driven engineering and formal methods.

The paper [6] proposes a pragmatic solution to guarantee security of a network of computers that supports the distribution of safety functions along a railway line.

The width of the issues addressed by the five contributions gives, we believe, a sufficient base for a deep discussion of the important challenges the research community has to address in the next years for what concerns future railway systems.

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 of the application of formal techniques to the distributed systems of systems represented by the future railway signalling systems.

References

1. Canonico, R., Flammini, F., Marrone, M., Vittorini, V., Nardone, N., Automatic generation of domain-aware control plane logic for software defined railway communication networks. In this volume.
2. 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). doi:10.1007/978-3-319-47169-3_18
3. Fantechi, A., Flammini, F., Gnesi, S.: Formal Methods for Intelligent Transportation Systems. 5th International Symposium, ISoLA 2012, Part II, Lecture Notes in Computer Science vol. 7610, pp. 187-189, Springer (2012). doi:10.1007/978-3-642-34032-1_19
4. Fantechi, A., Gnesi, S., Haxthausen, A.E., Formal Methods for Distributed Computing in Future Railway Systems, ISoLA 2020, Part III, Lecture Notes in Computer Science, vol. 12478, pp.389–392, Springer (2020). doi:10.1007/978-3-030-61467-6_24
5. Fantechi, A., Gori, G., Gnesi, S., Future train control systems: challenges for dependability assessment. In this volume.
6. Lecomte, T. Safe and Secure Architecture Using Diverse Formal Methods, In this volume.
7. Seisenberger, M., H. ter Beek, M., Ferrari, A., Haxthausen, A., James, P., Lawrence, A., Luttik, B., van de Pol, J., Wimmer, S., Safe and Secure Future AI-Driven Railway Technologies: Challenges for Formal Methods in Railway. In this volume.
8. Peleska, J., Haxthausen, A.E., Lecomte, T., Standardisation Considerations for Autonomous Train Control. In this volume.