Formal Verification of the Danish Railway Interlocking Systems

Vu, Linh Hong; Haxthausen, Anne Elisabeth; Peleska, Jan

Published in:
Pre-proceedings of 14th International Workshop on Automated Verification of Critical Systems (AVoCS 2014)

Publication date:
2014

Document Version
Publisher's PDF, also known as Version of record

Citation (APA):
Vu, L. H., Haxthausen, A. E., & Peleska, J. (2014). Formal Verification of the Danish Railway Interlocking Systems. In M. Huisman, & J. van de Pol (Eds.), Pre-proceedings of 14th International Workshop on Automated Verification of Critical Systems (AVoCS 2014) (pp. 257-258). University of Twente. (C T I T Workshop Proceedings Series; No. WP 14-01).

Formal Verification of the Danish Railway Interlocking Systems

Linh H. Vu[1]**, Anne E. Haxthausen**[1]**, and Jan Peleska** [2]

[1] DTU Compute, Technical University of Denmark, Denmark
[2] Department of Mathematics and Computer Science
University of Bremen, Germany

Abstract: In this paper, we present a method for formal verification of the new Danish railway interlocking systems. We made a generic and reconfigurable model of the behaviors and high-level safety properties of non-collision and non-derailment. This model accommodates *sequential release* – a new feature in the new Danish interlocking systems. Instantiating the generic model with interlocking configuration data results in a concrete model and high-level safety properties. Using bounded model checking and inductive reasoning, we are able to verify safety properties for model instances corresponding to railway networks of industrial size.

Keywords: railway interlocking systems, formal verification, bounded model checking, k-induction, safety-critical software systems, RobustRails

Introduction. An interlocking system is responsible for guiding trains safely through a given railway network. It is a vital part of any railway signaling system and has the highest safety integrity level (SIL4) according to the CENELEC 50128 standard [CEN11]. Conventionally, the development and verification process of interlocking systems is informal and mostly manual, hence time-consuming, costly, and error-prone. As part of the RobustRails research project[1], our work aims at establishing a holistic method supporting such a process. The method should be formal and facilitate automation in order to provide a better development and verification process compared to the conventional one. In Denmark, in the period of 2009–2021, new interlocking systems that are compatible with ETCS Level 2 [ERT12] will be deployed in the entire country within the context of the Danish Signalling Programme[2]. In the context of the RobustRail project accompanying the signalling programme on a scientific level, the proposed method will be applied to these new systems.

Figure 1 shows the verification process of our proposed method. The process begins with the configuration data [VHP14] in XML of an interlocking system consisting of: (i) a railway network layout specifying the geographical information of the railway network, and (ii) an interlocking table specifying how routes must be set so that trains can travel safely through the network. This configuration data is then used to instantiate our generic behavioral model of the Danish interlocking systems, and its high-level safety properties of non-collision and non-derailment. The behavioral model accommodates *sequential release*, a new feature that provides the potential to increase the capacity of the network. For verification and validation (V&V), we follow the typical two-step approach. In the first step, the data validation is performed on the configuration data to ensure the well-formedness of the model. In the second step, for a given

[1] http://robustrails.man.dtu.dk
[2] http://uk.bane.dk/visArtikel_eng.asp?artikelID=6090

configuration data, the concrete high-level safety properties are verified for the concrete model instance using bounded model checking (BMC) in combination with inductive reasoning. If the model instance does not satisfy the properties, counter-examples will be generated. The method has been implemented as a tool-chain for verifying interlocking systems using the RT-Tester toolbox [Pel13] and its state-of-the-art SMT solver – SONOLAR.

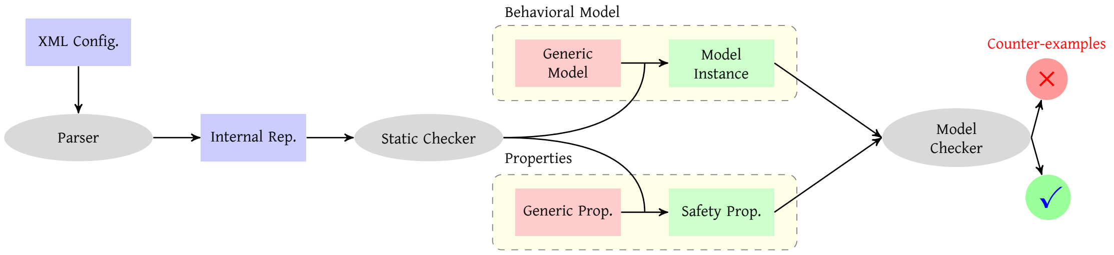

Figure 1: Verification Process

Experiments. We have successfully used the tool-chain to verify the safety properties for model instances of a number of railway networks, ranging from a trivial tiny toy network to a large station (Køge) extracted from the early deployment line of the new Danish signalling systems. The results demonstrate the advantages of the combined approach of BMC and inductive reasoning for verification of safety properties. First, it allows errors to be spotted quickly. Our experiences with BMC show that the counter-examples, if there are any, are found within a relatively short time of the model checking process. Second, the method can be scaled up to the size of real applications in practice, hence facilitating the automated V&V process of interlocking systems.

Bibliography

[CEN11] E. CENELEC. 50128 - Railway Applications-Communication, Signalling and Processing Systems-Software for Railway Control and Protection Systems. *Book EN 50128 Railway Application-Communications, Signalling and Processing Systems-Software for Railway Control and Protection Systems*, 2011.

[ERT12] ERTMS. Annex A for ETCS Baseline 3 and GSM-R Baseline 0. April 2012. http://www.era.europa.eu/

[Pel13] J. Peleska. Industrial-Strength Model-Based Testing - State of the Art and Current Challenges. In Petrenko and Schlingloff (eds.), Proceedings 8th Workshop on Model-Based Testing. Electronic Proceedings in Theoretical Computer Science 111, pp. 3–28. Open Publishing Association, 2013.

[VHP14] L. H. Vu, A. E. Haxthausen, J. Peleska. A Domain-Specific Language for Railway Interlocking Systems. In Schnieder and Tarnai (eds.), *FORMS/FORMAT 2014 Proceedings*. To appear online by Elsevier, 2014.