Formal Development and Verification of Railway Control Systems

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

Publication date:
2013

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

RobustRails

Formal Development and Verification of Railway Control Systems

Linh Vu Hong1, Anne Haxthausen1, and Jan Peleska2
1DTU Compute, Technical University of Denmark
2Department of Mathematics and Computer Science, Bremen University

This paper presents work package WP4.1 of the RobustRails research project. The work package aims at suggesting a methodology for efficient development and verification of safe and robust railway control systems.

1 Project background and state of the art

Over the next 10 years all Danish railway signalling systems are going to be completely replaced with modern, computer based railway control systems based on the European standard ERTMS/ETCS [3, 4] by the Danish Signaling Programme [1]. The purpose of these systems is to control the railway traffic such that unsafe situations, like train collisions, are avoided. Central parts of these new systems consist of safety-critical software the functional correctness of which is one of the key requisites for a reliable operation of the traffics and in particular for the safety of passengers. Until now the development of railway control software has typically been done applying conventional methods where requirements and designs are described using natural language, diagrams and pseudo code, and the verification of requirements has been done by code inspection and non-exhaustive testing. These techniques are not sufficient, leading to errors and an in-effective and costly development process. The railway sector and in particular Rail Net Denmark (Banedanmark) therefore call for improved software development methods.

2 Original contribution and expected results

In order to avoid the problems mentioned in previous section, it is strongly recommended by the CENELEC standards [2] for railways to use formal (i.e. mathematical) logic and models for the unambiguous description of requirements and designs as well as for exhaustive verification as they give a higher assurance of safety compared to conventional methods. The use of domain-specific methods is another trend in software development, suggested to make the construction of software more efficient by generating the software automatically from domain-specific descriptions. Hence, to combine these two approaches is expected to be very attractive. The project will examine how domain-specific methods and formal methods can be combined and used for an efficient development and verification of new fail-safe systems. The expected result is a methodology for using domain-specific, formal languages, techniques and tools for more efficient development and verification of robust software for railway control systems. The hypothesis is that domain-specific, model-based system development methods will lead to a more efficient construction with fewer errors and these errors will be found earlier in the system development.

3 Acknowlegments

This work is part of the research project RobustRails funded by the Danish Council for Strategic Research. The work is affiliated with a number of partners: DTU Compute, DTU Transport, DTU Management, DTU Fotonik, Bremen University, Banedanmark, Trafikstyrelsen, DSB, and DSB S-tog. More information about RobustRails project is available at http://www.dtu.dk/subsites/robustrails/English.aspx

References

[1] Banedanmark. The Signaling Programme - A total renewal of the Danish signaling infrastruture. 2010.
[2] E.N. 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, 2012.
[3] ERTMS. Annex A for ETCS Baseline 3 and GSM-R Baseline 0, April 2012.
[4] P. Stanley. ETCS for Engineers. Eurailpress, 2011.