Formal modelling and verification of interlocking systems featuring sequential release - DTU Orbit (14/09/2019)

Formal modelling and verification of interlocking systems featuring sequential release
In this article, we present a method and an associated toolchain for the formal verification of the new Danish railway interlocking systems that are compatible with the European Train Control System (ETCS) Level 2. We have made a generic and reconfigurable model of the system behaviour and generic safety properties. This model accommodates sequential release - a feature in the new Danish interlocking systems. To verify the safety of an interlocking system, first a domain-specific description of interlocking configuration data is constructed and validated. Then the generic model and safety properties are automatically instantiated with the well-formed description of interlocking configuration data. This instantiation produces a model instance in the form of a Kripke structure, and concrete safety properties expressed as invariants. Finally, using a combination of SMT based bounded model checking (BMC) and inductive reasoning, it is verified that the generated model instance satisfies the generated safety properties. Using this method, we are able to verify the safety properties for model instances corresponding to railway networks of industrial size. Experiments show that BMC is also efficient for finding bugs in the railway interlocking designs. Additionally, benchmarking results comparing the performance of our approach with alternative verification techniques on the interlocking models are presented.

General information
Publication status: Published
Organisations: Software and Process Engineering, Department of Applied Mathematics and Computer Science, University of Bremen
Contributors: Vu, L. H., Haxthausen, A. E., Peleska, J.
Pages: 91-115
Publication date: 2017
Peer-reviewed: Yes

Publication information
Journal: Science of Computer Programming
Volume: 133
ISSN (Print): 0167-6423
Ratings:
BFI (2017): BFI-level 2
Scopus rating (2017): CiteScore 1.24 SJR 0.3 SNIP 1.034
Web of Science (2017): Impact factor 0.74
Web of Science (2017): Indexed yes
Keywords: Railway interlocking systems, Sequential release, Formal verification, Bounded model checking, k-Induction
Electronic versions:
2016.2main.pdf. Embargo ended: 26/05/2018
DOIs:
10.1016/j.scico.2016.05.010
Source: FindIt
Source ID: 2304879469
Research output: Contribution to journal › Journal article – Annual report year: 2016 › Research › peer-review