Science of Computer Programming ••• (••••) •••–•••

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

Verification of the European Rail Traffic Management System in Real-Time Maude

Ulrich Berger [a], Phillip James [a], Andrew Lawrence [b], Markus Roggenbach [a], Monika Seisenberger [a,*]

[a] Swansea University, Swansea, UK
[b] Siemens Rail Automation UK, Chippenham, UK

ARTICLE INFO

Article history:
Received 24 July 2016
Received in revised form 30 September 2017
Accepted 20 October 2017
Available online xxxx

Keywords:
Railway signalling
ERTMS/ETCS
Hybrid systems
Real-Time Maude
Model-checking

ABSTRACT

The European Rail Traffic Management System (ERTMS) is a state-of-the-art train control system designed as a standard for railways across Europe. It generalises traditional discrete interlocking systems to a world in which trains hold on-board equipment for signalling, and trains and interlockings communicate via radio block processors. The ERTMS aims at improving performance and capacity of rail traffic systems without compromising their safety.

The ERTMS system is of hybrid nature, in contrast to classical railway signalling systems which deal with discrete data only. Consequently, the switch to ERTMS poses a number of research questions to the formal methods community, most prominently: How can safety be guaranteed? In this paper we present the first formal modelling of ERTMS comprising all subsystems participating in its control cycle. We capture what safety means in physical and in logical terms, and we demonstrate that it is feasible to prove safety of ERTMS systems utilising Real-Time Maude model-checking by considering a number of bi-directional track layouts.

ERTMS is currently being installed in many countries. It will be the main train control standard for the foreseeable future. The concepts presented in this paper offer applicable methods supporting the design of dependable ERTMS systems. We demonstrate model-checking to be a viable option in the analysis of large and complex real-time systems. Furthermore, we establish Real-Time Maude as a modelling and verification tool applicable to the railway domain.

The approach given in this paper is a rigorous one. In order to avoid modelling errors, we follow a systematic approach: First, as a requirement specification, we identify the event-response structures present in the ERTMS. Then, we model these structures in Real-Time Maude in a traceable way, i.e., specification text in Real-Time Maude can be directly mapped to requirements. We explore our models by checking if they have the desired behaviour, and apply systematic model-exploration through error injection – both these steps are carried out using the formal method Real-Time Maude. Finally, we analyse ERTMS by model-checking, thus applying a formal method to the railway domain, and we mathematically prove that our analysis of ERTMS by model-checking is complete, i.e., that it guarantees safety at all times.

* Corresponding author.
E-mail address: m.seisenberger@swansea.ac.uk (M. Seisenberger).

https://doi.org/10.1016/j.scico.2017.10.011
0167-6423/

Please cite this article in press as: U. Berger et al., Verification of the European Rail Traffic Management System in Real-Time Maude, Sci. Comput. Program. (2017), https://doi.org/10.1016/j.scico.2017.10.011

1. Introduction

In 2004, the 18th IFIP World Computer Congress identified the railway domain as a Grand Challenge of Computing Science [20] because it is of immediate concern and because it also provides a set of generic, well-understood problems whose solutions would be transferable to various other application domains, e.g., process control in manufacturing, also known as industry 4.0.

1.1. The development of ERTMS

Reflecting on the concerns arising out of this Grand Challenge, the following are recurring statements from the 2007 Department of Transport White Paper "Delivering a Sustainable Railway" [8]:

- "Rail's biggest contribution to tackling global warming comes from increasing its capacity."
- "Reliability and capacity are amongst top passengers' concerns."
- "Increasing capacity is the most urgent investment need."

The European Rail Traffic Management System (ERTMS)/European Train Control System (ETCS) is a signalling, control and train protection system developed to address these issues. It is designed to allow for high-speed travel, to increase capacity, and to facilitate cross-border traffic movements [10]. ERTMS/ETCS is a complex system of systems, made up of several distributed components. It is specified at four different levels, each of which defines a different use as a train control system. In our paper we consider ERTMS/ETCS Level 2, which is characterised by continuous communication between trains and radio block centres.

With the introduction of ERTMS a number of research questions arise: How can safety be guaranteed? How can reliability and performance be measured and estimated? How can capacity be measured and improved? Behind these questions are, from a computer science point of view, long-standing research challenges: how can we effectively perform qualitative and quantitative reasoning on complex systems?

- Qualitative reasoning is required to ensure safety.
- Quantitative reasoning is needed to measure both capacity and reliability.

In our paper, we provide a model of ERTMS Level 2 which we qualitatively analyse for safety using timed model-checking. It is, however, also open to quantitative analysis via simulation, for example, for studying rail network capacity (e.g. how many trains can be observed in the network within a given period of time) or exploring energy consumption (e.g. a slow train may force a faster following train to make regular speed adaptations leading to high energy consumption).

1.2. Formal methods in the railway domain

Industrial standards for railway and related domains are increasingly relying on the development of formal methods for system analysis in order to establish a design's correctness and robustness. Recent examples include the 2011 version of the CENELEC standard on railway applications, the 2011 ISO 26262 automotive standard, or the 2012 Formal Methods Supplement to the DO-178C standard for airborne systems.

Fantechi [11] begins his 2014 survey on formal methods in the railway domain: "Since more than 25 years, railway signalling is the subject of successful industrial application of formal methods in the development and verification of its computerised equipment". In this context, especially the verification of *interlocking systems* has played an important role. An interlocking system is responsible for guiding trains safely through a given railway network. It is a vital part of any railway signalling system and has the highest safety integrity level (SIL4) according to the CENELEC 50128 standard.

1.3. Classical interlocking designs

It is still an open research question as how to perform formal safety checks on interlocking designs. The challenge is how to cope with the complexity of the problem: the state space grows exponentially in the size of the scheme plan to be verified. Several research groups, see e.g. [19,3,17,13,15,14,24,23,22,12,18,39,38,36,4,28], have been addressing this challenge and have developed a number of different modelling and verification approaches.

The modelling part of such approaches usually consists of "transformations" that aim to derive a (formal) model from informal rail descriptions as used in rail industry, such as a track plan (e.g., as a CAD drawing) enriched by various tables (e.g., control tables). Similarly, the verification part usually states a safety condition (e.g., no train collision) and expresses this as a (formal) property (e.g., as a logical formula). Finally, an (automated) verification tool is utilised to provide an answer whether or not the property holds in the model. It is an open research question of how to compare such models and verification methods. As a first step in this direction, Haxthausen et al. [16] discussed the challenges, provided first steps towards a general method to compare these approaches, and performed an initial, however systematic, comparison between two of the above mentioned approaches.

Please cite this article in press as: U. Berger et al., Verification of the European Rail Traffic Management System in Real-Time Maude, Sci. Comput. Program. (2017), https://doi.org/10.1016/j.scico.2017.10.011