Abstract: Formalization of operational regulations for railways (hEART 2018)

Sebastian Schön[1], Eduard Kamburjan[2], Andreas Oetting[1], Reiner Hähnle[2]

[1] Railway Engineering Group, Technische Universität Darmstadt

[2] Software Engineering Group, Technische Universität Darmstadt

1 Introduction

Today operational rules are collected in rulebooks that are manually created and maintained. This can result in specification gaps and in ambiguities. We develop a method for uniform modelling of railway operation procedures and their rules to obtain executable, formal models of current and future railway operation procedures. Such models can be used to accelerate planning and approval processes. They also have the potential to increase network capacity through a fine-grained analysis of the interactions between operational procedures and the infrastructure. The total reduction of operation costs in future operational scenarios makes formal modelling an important tool for railways to stay competitive.

The research group “AG Signalling”, part of the strategic cooperation between TU Darmstadt and Deutsche Bahn (Europe's largest railway operator and railway infrastructure manager), works on the latest generation of interlocking systems and future railway operation procedures.

One of the projects pursued in AG Signalling, the FormbaR-Project[2], formalizes operational and other rulebooks of railways. In the following we present the general modelling approach and the usage of a modelling language that supports verifiable specifications, executable models and has an unambiguous, formal semantics. This constitutes a novel alternative to modelling railway operation procedures that opens up the path for using advanced software analysis tools in the railway domain.

To validate our models, we base them on real railway infrastructure data, so as to simulate actual operational scenarios. These scenarios include regular train operation as well as operation in the event of deviations.

Since our models have a formal semantics and take the form of an executable software program, they do not only permit simulation, but also formal verification: existing software verification tools allows to mathematically prove the safety of operational procedures, independently of a concrete infrastructure.

2 Railway operation rules and procedures in Germany

The very long braking distances caused by the low static friction between wheel and rail are one reason why railways are controlled and regulated more strictly than road traffic. In particular, the possible movements of all vehicles in a given area is considered. This historically includes the operation of point machines, train detection devices and signals separating train movements. Driving on sight is the norm during shunting movements – for normal train movements, driving on sight is only used in the event of deviations, e.g. for passing a malfunctioning signal.

1 corresponding author: schoen@verkehr.tu-darmstadt.de

2 www.formbar.raillab.de/en

This results in a situation where all aspects of railway operations are governed by laws and regulations issued by the Federal Government, as well as by rulebooks written by the corporation managing the infrastructure.

The rulebooks can be grouped by their purpose into three main categories:

- Planning, building and maintenance of railway infrastructure
- Planning of railway operations (e.g. Timetables)
- Rulebooks for railway operations

This paper deals with the latter category: rulebooks for railway operations; however, minor adaptions allow for a use for rulebooks of the other above-mentioned categories.

3 Creation and maintenance of rulebooks for railway operations

The current rules for railway operations are based on over 100 years old rulebooks, dating back to 1907 in Germany. Changes to these rulebooks may be necessary because of changing laws, following reactions on incidents, motivated by feedback from users (e.g. infrastructure planners or train dispatchers) or as a consequence of the introduction of new technologies for the control of train movements (e.g. ETCS).

Feedback from users mostly originates from ambiguous rules, one of the main problems when rules are written in natural language. This was also one of the main findings in an interview series conducted with experienced rulebook authors working for the infrastructure manager DB Netz AG at the start of our research in 2016. A *formal* model of railway operations would allow to create a redundancy-free, unambiguous set of rulebooks. Other advantages, which we identified during the interviews, and that we will address in detail during our presentation, are:

- Access to all necessary regulatory content
- Possibility of visualization
- Automated maintenance of dependencies and cross references
- Detection of redundancies or gaps in specifications
- Simulation runs to help the process of designing rules and regulations
- Formal proof of safety properties
- Abandonment of natural language version in selected cases

In the following, we present the steps undertaken towards our formal model of railway operations, starting with the railway operation procedures, followed by models for infrastructure and trains.

4 Modelling operational procedures with ABS

Our modelling approach uses the Abstract Behavioral Specification (ABS) language as a novel alternative to modelling railway operation procedures. ABS has been created in a series of EU projects by European universities starting from 2009, with a particular focus on combining usability, executability and verifiability [1]. The syntax is loosely based on Java. During their university training many engineers become familiar with Java or related object-oriented programming languages, such as C++.

By means of a small example, the good comprehensibility of the formal ABS model shall be demonstrated. The example below shows the railway operation procedure after stopping a train in front of a defective signal which cannot signal “stop” any more. Once the affected train comes to a stop at

the signal, a list of written orders must be processed. Anyone familiar with the operational rules laid down in the rulebook can immediately see that the code in Figure 1 directly represents them.

```
Unit handleTrainBeforeBrokenSignal(Signal s){
        Train train = await s!getObserver();
        await train!acqStop();
        train!order(list[order144,order2]);
}
```

Figure 1: Code Example

The FormbaR-Project works on the uniform modelling of a set of railway operation procedures of the rulebook 408, which is issued by DB Netz AG and includes all the processes concerning train movement and shunting. In the presentation, we will demonstrate a user-friendly method to model new procedures and scenarios.

To validate the model, we utilise operational scenarios and simulation runs during the process of modelling the railway operation procedures and carry them out on models of the actual infrastructure with real train data. Our infrastructure model is presented below.

5 The FormbaR railway infrastructure model

We model the infrastructure, i.e. track elements, as a layered model centred around *points of information flow*. A point of information flow is a position on the track, where information from or to a train may be transmitted. The use of an undirected graph with points of information flow as nodes guarantees flexibility (e.g. adding new infrastructure elements) and a redundancy-free representation.

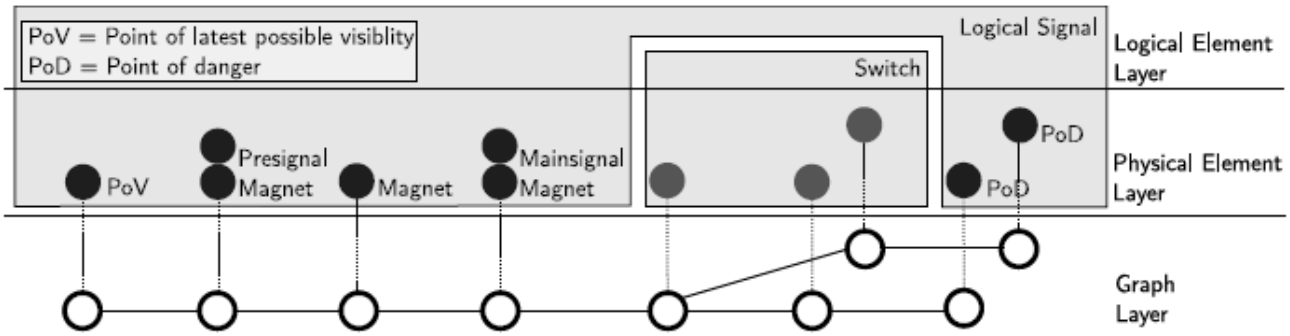

Figure 2: An example of an entry signal in the FormbaR railway infrastructure model

Multiple *physical* elements can be associated with a single point of information flow. Multiple physical elements such as the main signals, the pre-signals that indicate to the train driver the state of the upcoming main signal, and infrastructure elements of the train protection system can be grouped into *logical* elements. This reflects the structure of the rulebooks. For example, when the rulebook describes the actions to change the state of a main signal, implicitly the state of its pre-signal and the functions of the train control systems are included.

The FormbaR model simplifies certain aspects of train operation: E.g., the actions of the train driver are modelled to be fault-free. This is not a principal limitation: Other projects in the research group “AG Signalling” address some of these simplifications at the moment: E.g., driverless operations during deviations. The joint work on the model will make it possible to cover numerous scenarios in the future.

While our models may be executed and used for simulation, the formal semantics of ABS also makes it possible to formally verify that the modelled procedures are safe, for an *abstract, unlimited* infrastructure.

6 Beyond Simulation: Formal Proofs

The communication protocol that forms the basis for the operational procedures gives rise to a mathematical structure. This structure is used to analyse all possible states of the infrastructure and the trains – however, we are not required to analyse each state in isolation, but can reason about unbounded traces of states. This reasoning about traces makes it possible to mathematically verify procedures for any, i.e. for *arbitrarily big* infrastructures with the use of the KeY-ABS tool [2, 3].

Our first formal verification was the permit token exchange described in the rulebooks. That study showed that the effort for such proofs is feasible.

7 Literature

[1] Einar Broch Johnsen, Reiner Hähnle, Jan Schäfer, Rudolf Schlatte, Martin Steffen: ABS: A Core Language for Abstract Behavioral Specification. FMCO 2010: 142-164

[2] Eduard Kamburjan, Reiner Hähnle: Uniform Modeling of Railway Operations. Formal Techniques for Safety-Critical Systems 2016: 55-71

[3] Eduard Kamburjan, Reiner Hähnle, Sebastian Schön: Formal Modeling and Analysis of Railway Operations with Active Objects. To appear in: Science of Computer Programming