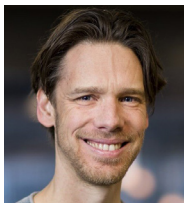
IRSE
Institution of Railway Signal Engineers

The use of formal methods in standardisation of interfaces of signalling systems






Prepared on behalf of the International Technical Committee by Maarten van der Werff, Bernd Elsweiler, Bas Luttik and Paul Hendriks

Like other infrastructure managers (IMs), ProRail BV and DB Netz AG are responsible for the safe and efficient running of trains; their signalling systems play an essential role in this task. That is why they have to convince themselves of the correct level of safety of the technology used. This article describes the cooperation of these two IMs in paving the way towards the application of formal methods that can be used to prove the quality of software applied in signalling. As described later in this article, the scope of the work focuses on the interfaces within the signalling system.

This paper about interlocking interfaces is one of three ITC articles concerning formal methods. The second will address the use of formal methods in the certification process of Hybrid Level 3 ETCS, the third will deal with interlocking applications.

Signalling domain specific requirements

Many railways do not have a complete written set of signalling system requirements readily available. A lot of knowledge is still in the minds of a few specialists; technical solutions and schemes that are common to conventional technology are available; specialists know how to read their own documents. It is routine that in specification, review and validation specialists communicate in natural language. However in the interlocking domain this information is incomplete and ambiguous.

A complicating factor is that the signalling requirements include the operational rules of railway undertakings. In the course of time, this has been implicitly assessed by the agreement of the captured requirements for conventional interlockings. For a correct interpretation needed in the digitalisation of signalling and communications technology the implicit operational background must be made more explicit. The analyses of use cases based on railway operations should lead to an unambiguous description of functionality and behaviour of the system to be designed. An unambiguous description cannot be achieved using natural language, on the contrary, the development of reliable computer technology in the modern signalling environment requires the use of state-of-the-art methods and tools. Tooling is often associated with high investment costs. It is, therefore, preferable to collaborate on an international level and use standardised methods and techniques tailored for the signalling industry.

History of formal methods in signalling standardisation

In 1997 the UIC published the report of the European Railway Research Institute (ERRI) project A201 proposing to harmonise functional conditions of signalling systems. For the first time in signalling history the functional rules of interlockings were exchanged and analysed on a very broad basis. This was supposed to be a future proof approach, because even if new signalling technology were to appear, the basic vital functionalities would continue to exist. A more formal way of describing the interlocking functional requirements was sought, but this could not be found. In those days no cost-effective common approach was applied across the railways or in industry. This is still what we do, but we are far better at analysing state-transition diagrams nowadays, and we have higher-level languages to describe them.

As there was not much experience with formal and semi-formal methods many new methods were developed. In the UIC working group UIC 7A/16 a method called EURIS (European Railway Interlocking Specification) was developed. The EURIS method is a semi-formal method that defines building blocks (e.g. Signal, Track, Point). For each building block, operations are defined and these operations are described using flow charts.

In the UIC-project EURO-INTERLOCKING (1998-2008) for one of the first times ever a systematic approach was exercised for translating the captured requirements

into a model, and that model was visualised with a tool. It appeared that both the skills of a signal engineer and a modelling specialist were needed to do this work. Besides this, during modelling it was experienced that in an iterative process the requirements needed an extra quality step both in verbal language and in completeness.

Based on the EURO-INTERLOCKING experience, in INESS (Integrated European Signalling System, 2008-2011) it was decided to define work for universities both for modelling and for exercising consistency checks. The objective of INESS was to develop specifications and associated material for the development of a European interlocking standard based on common requirements, including ways to verify models for interlockings. Tools to be used were defined, taking into account that there was a limited budget, that needed to reuse and modify existing tools, rather than develop new ones. The result of INESS contained a verification tool chain in the form of a research prototype, which could lead to a modelling and verification environment. However the model became available only towards the end of the project, when there was no time left for in-depth verification activities.

Model based system engineering

An important development evolved in EULYNX (project phase 2013- 2017, continuing organization from 2017 onwards **www.eulynx.eu**). In EULYNX the European infrastructure managers standardise the interfaces between signalling subsystems of different suppliers. The adoption of EULYNX will reduce both life cycle costs and time-to-market by preventing repetitive industrial developments of interface technology. EULYNX has developed a reference architecture, including how subsystems interact across the interlocking interfaces. EULYNX uses model-based system engineering (MBSE) which means that the functional behaviour of the interfaces is defined through unambiguously semi-formal, executable models. This complies with the CENELEC standard EN50128, which states that semi-formal methods are highly recommended for the specification of software requirements.

EULYNX is an innovative way in comparison with specifying requirements in natural language. The (semi-) formal method can be understood by people, and offers the user multiple views of the system to allow a clear understanding. Using the SysML modelling method, the infrastructure managers have defined the appropriate use case descriptions based on their knowledge of both national signalling principles and the non-harmonised operational requirements.

Following the experience from EURO-INTERLOCKING and INESS, in this phase modelling and system engineering expertise is combined with railway expertise. In recent years modelling has been accepted in various fields, such as the chemical, automotive, aerospace and telecom industries. This method includes the test domain by introducing model based testing. The method for modelling interfaces in combination with model based testing and generation of automatic test cases will be crucial for maintaining the standard. Early feedback that the standard is compliant with the automation of test execution will increase the level of sustainability. This is a prerequisite for keeping the standardised interfaces alive.

Implementation phase at IMs

A feasibility study conducted research on EULYNX models and the specifications that were available at ProRail. It included reviewing the modelling domain. This led to the conclusion that the EULYNX form of modelling can be useful for ProRail. It helps to understand the interface communication between interlocking and its subsystems. For example, EULYNX requirement specifications contain the main information in the form of models, while ProRail does not have models that describe these requirements.

DB Netz has already gone one step further in applying standardised interfaces in signalling projects. Starting with a national specification project some years ago, DB adopted the first European specifications in their latest projects and will use the European specifications for their roll-out programme. This approach delivers clear added value with respect to life cycle costs, innovation and performance objectives of future signalling systems.

Since EULYNX uses the concept in which the model is the main container of the requirements, the validation process is mainly the validation of models. It is the basic task of each IM to create a validation and testing approach to ensure that all requirements are included for implementation. With the already published baseline EULYNX has taken an important step towards formulating a stable standard. This result is sufficient to enforce an unambiguous interpretation by various suppliers. Validated SysML models provide useful guidance when testing the conformity of delivered components to the IM.

Current initiative of ProRail and DB Netz

Infrastructure managers DB Netz AG and ProRail together with Eindhoven University of Technology and the University of Twente have decided to investigate the use of formal models in a research project called FormaSig. Formal models are models that are defined in a formal modelling language with mathematical semantics that can be fully understood by a computer. These two universities have developed a formal modelling language and a corresponding powerful tool set, which are particularly suitable for analysing the quality of the system designs. They will perform a mathematical proof that the interfaces behave correctly, based on the EULYNX SysML models, national knowledge and the typically used national specific subsystems of the two infrastructure managers. You can watch a presentation of this project on YouTube at **irse.info/6dujm**.

The main objective of the research project is to encourage the use of (formal) models in order to improve the quality of standards and tender documents in the railway domain. An explicit concern of the IMs is the traceability of requirements formulated in natural language. With the increasing complexity of today's electronic signalling systems, it becomes increasingly difficult to verify that they meet their original requirements. However, the methods developed in this project will help to define test specifications that allow interfaces to be validated without full traceability to legacy requirements. The result will be that experts are exposed to a new way of working with regard to specification, testing and certification in the relation to market parties.

The results of the project can support the EULYNX standardisation process in the entire chain from users to equipment, including the approval processes for interfaces to supplied components. The development of the EULYNX standard provides an excellent opportunity to investigate how this approach based on semi-formal and formal models can further improve the applicability and the scalability of methods applied in the railway domain, as well as industrial verification and testing of state-of-the-art academic technologies.

We know from the past that development of a formal method requires a lot of resources (time, money). This experience was built on interlocking modelling in INESS. By limiting the scope to interfaces, which contain much less functionality compared to a complete interlocking

(even with a limited number of field elements), it is expected that the project ambition will be achieved within the foreseen period of four years and for acceptable costs.

Benefit for the interlocking domain

The use of formal methods in the standardisation of interfaces of signalling systems is a continuation of long-term use of knowledge of (semi-) formal methods. This had already begun with the introduction of the Vital Processor Interlocking of General Railway Signalling in the Netherlands in the 1990s. This knowledge has been an input for the European standardisation projects mentioned above. It has been shown that many experts and students involved have found their careers in the field of railway signalling.

Formal methods will help to accelerate innovation processes and establish standards at a European level. In particular formal representations of real systems help to develop and test new functions applying state of the art engineering tools. For industry as well as for IMs formal methods are the basis for the automation of test procedures and are therefore helpful means to maintain international standards.

By continuing the cooperation between IMs and universities the circle of knowledge carriers will receive a new impetus. As was seen in the 1990s it can be expected that the initiative of ProRail and DB will also result in more activities in the combined knowledge domain of electronic interlockings and modelling, both for the railways and for market parties. In future a new generation of signalling experts working in the signalling domain will apply the results of the initiatives described. These experts will be exposed to a new way of working with regard to specification, testing and certification in relation to market parties. Suppliers already have their own system design processes and all these known and unknown steps need to be linked in the right way. Railways must invest resources in this type of activity. Consultants and engineering services in the area of (semi-) formal specification and universities can work on that task in order to get sufficient state-of-the-art skills in the process.

Conclusion

The characteristics of railways have made it necessary to introduce complex systems for signalling to avoid essential hazards. The aim is to improve the competitiveness of the railway business. The formal methods developed in the research project will help to define test specifications with which signalling systems can be validated without full traceability to legacy requirements. The initiative of ProRail and DB shows that 25 years of effort in the area of standardisation offers advantages in the field of effective and efficient quality improvement in the specification, realisation and validation of signalling systems.

All the IMs involved in EULYNX can benefit from the results by using the methodology and tools in their own quality assurance processes.

The ITC and the authors thank ProRail, DB, and the involved universities that contributed to this article.

About the authors

Maarten van der Werff is Manager, Expert Group Interlocking, Prorail BV, Netherlands.

Bernd Elsweiler is Head of Digital Signalling, DB Netz AG, Germany.

Bas Luttik is Assistant Professor, Department of Mathematics and Computer Science, Eindhoven University of Technology, Netherlands.

Paul Hendriks is Manager Signalling, ProRail BV, Netherlands.