Moving Safely Towards IP Protocol for Signalling Equipment

João Martins, Software Development Leader, EFACEC
José Fonseca, Product Manager, EFACEC

SUMMARY

In railway systems, the trackside equipment represent an important layer for signalling solutions, the one responsible for the interaction with the physical world, i.e., the one responsible for lighting a lamp to show a proceed aspect to a train or to detect a train within an area. The interface with this layer is changing, as electrical interfaces are being replaced by communication protocol interfaces. In fact, hardware interfaces are being replaced by software interfaces. This replacement is mainly explained by the efficiency of SW systems regarding data exchange, due to their high integration, flexibility, and scalable capability for large amounts data. The efficiency in (Big) data collection provided by communication protocols is essential when predictive maintenance systems are evolving fast with the goal to reduce maintenance costs and increase the systems life-cycle/resilience, or when an increase in the interoperability is required to improve the performance and reduce the development costs of railway systems.

The introduction of communication protocol interfaces raises new challenges concerning safety and security aspects, in order to ensure data integrity and authenticity, respectively. The EN 50159 identifies the threats that a transmission system is subjected to, as well as defence strategies for the identified threats in the attempt of tackling safety and security issues. Regarding RAM (Reliability, Availability and Maintainability) even though they were not addressed by EN 50159 they should also be re-evaluated with this new type of interface in mind. Despite the mentioned challenges, there are already several communication protocols being successfully used by trackside equipment to exchange safety-related data. However, there is still not a consensual standard protocol despite the effort of projects like EULYNX. As a consequence, a new set of protocols had emerged, pushed by the appearance of new IP equipment.

The new vague of safety protocols entails also a challenge to system integrators, the implementation of these protocols. Thus, this paper presents an approach for the development of safety protocols intended to be compliant with EN50128 for SIL 4 systems. The approach follows a model-based development process, targeting the creation of a formal model with the aim to assess the protocols safety properties. In order to reduce unnecessary complexity and (consequently) improve the probabilities of a successful formal verification process, only the safety functions should be considered for the model creation, while the remaining functions (ex: socket management) should be added in the final target system. An implementation of the safety protocol FSE (Frauscher Safe Ethernet) will be developed following the proposed approach in order to validate it against an already certified safety protocol for category 2. Hence, while demonstrating the power of the modelling process, this paper also illustrates the importance of conducting formal proofs to ensure the safety properties of protocols, with the reuse of these properties in mind since most of the safety mechanisms provided by protocols are the same.

1 INTRODUCTION

The communication protocols will have a key role in the future of railway systems, essentially due to the digitalization of railway industry and the consequent massification of equipment's supporting an IP interface. Arguably, one of the most prominent challenges for communication protocols in the future of railway is related with software development, more precisely, with the implementation of safety communication protocols.

This paper presents an approach for the development of safety protocols intended to be compliant with EN50128 for SIL 4 systems. The approach follows a model-based development process, targeting the creation of a formal model with the aim to assess the protocols safety properties. Considering the potential complexity of complete system and the computational effort involved in formal verification, only the safety functions are considered for the model. This strategy not only reduces the overall complexity of the model but also increases the probabilities of successfully completing the formal verification process in an acceptable time. The Frauscher Safe Ethernet (FSE) will be used as the case study to validate the mentioned approach, and so, its implementation will be performed

following the proposed development process. Hence, this paper intends to contribute for the demonstration of the modelling power and to highlight the relevance of formal methods concerning the verification of systems safety properties.

2 THE RELEVANCE OF IP PROTOCOLS IN THE FUTURE OF RAILWAY SYSTEMS

Ever since the introduction of electrical equipment in the field of railway signalling, information has been passed between systems using one pair of wires for each signal. This architecture, being simple and straightforward, was particularly well suited to the low quantities of information that needed to be transmitted by those early systems.

Although still in use by the railway industry throughout the world, wire-by-wire communication eventually became a bottleneck in the information exchange between railway signalling systems. Particularly with the introduction of computer-based systems, the amount of data to be exchanged lead to the introduction of serial communication, based on proprietary protocols. An example of such systems is the so-called data link used by Solid State Interlocking (SSI), introduced in the 1980s (Leach, 1991).

While representing a significant leap forward, data links were based on proprietary hardware, exchanging information in a predefined way. Data throughput, although responding to the requirements of the SSI, will be categorized by today's standards as modest, to say the least. The architecture of the system used dedicated point-to-point links between each pair of systems in need to communicate with each other.

Although the concept of packet switched networks was first introduced long before the first deployments of data links, when such networks became prominent in the 1990s there still had no direct use for real time applications. Only in the 2000s real time audio and video started to be massively transmitted over packed switched networks, mostly using Internet Protocol (IP).

After the described evolution, the aim of using serial protocols over packet switched networks can be seen as obvious. These networks are widely spread, being deployed in greenfield projects as well as a retrofit the existing infrastructure. Today's networks support incredibly high data rates and incorporate sophisticated redundancy mechanisms, resulting in high availabilities. The challenge, as we will describe, is to complement all this with the adequate level of safety.

2.1 Industry 4.0 and Rail 4.0

The massive introduction of cyber-physical systems, combining a physical component with a digital part, characterize the so-called Industry 4.0, or fourth industrial revolution. Modern railway signalling systems, being composed of field objects and interlocking software, fit quite well in the definition of cyber-physical systems.

The level of interaction between the cyber and the physical parts of signalling systems has greatly increased in the last years. Peripheral components, like signals and point machines, are being deployed with an increasing number of sensors, allowing the interlocking and related systems to receive far more field data than is the case with traditional systems. Such volumes of data are by no means compatible with wire-by-wire interfaces, being only efficiently exchanged using communication protocols.

The amount of data provided by the aforementioned sensors also provide valuable information for the maintenance of the systems. Knowing the trend of the provided measurements can, when analysed with the correct algorithms, predict the occurrence of failures before they become apparent. This kind of predictive maintenance can positively impact the overall cost of ownership of a system, by reducing the effort in preventive maintenance.

Not being specific to the railway industry, the described trends are aligned with its the current needs, giving birth to what is known as Rail 4.0. Although following the steps of Industry 4.0, Rail 4.0 is evolving slower, due to the traditionally conservative character of the railway industry, where innovations tend to be introduced later than in other industries. An example is the introduction of safety PLCs. Although now an established tendency, their introduction in the railway industry, particularly in signalling, occurred when other safety critical businesses had already widely adopted it.

The mentioned PLCs are a particular case of the use of Commercial Of The Shelf (COTS) equipment, meaning that no specific development is done to have components that are tailored for railway use. In fact, the safety concerns applicable to railway signalling are not significantly different from those found, for example, in nuclear or petrochemical domains.

2.2 Cybersecurity

The communication protocols play an important role in the digitalization of railway industry by providing the means for the communication between equipment's/systems. With increase of communication protocols use, also cybersecurity challenges will become more prominent, in particular, those referring to safety aspects. Thus, topics like the reliability of encrypted communications will become essential for the success of the mentioned digitalization process.

Cybersecurity challenges are being addressed by almost all industries and the railway sector is not an exception. In fact, this topic can be even more important for railway industry, since the segregated networks environments (closed networks), typically used in railway, may become less common due to the claim to reduce infrastructure costs and the need of a higher integration between railway systems and external systems. The foreseeable use of public 5G networks will be an additional factor of concern for these matters.

2.3 Interoperability

Being a niche market, with very specific and demanding requirements, the railway industry has traditionally privileged specific developments, most commonly to be used only by one railway administration. The evident impacts of this strategy are the need to start every development from scratch and the inability to interconnect sub-systems of different manufacturers or railway networks.

With the ever-increasing demand for performance, with the inevitable impact in system complexity, not being able to use components from other manufacturers has proved to be a source of inefficiency. Inversely, no stimulus existed for smaller companies to develop building blocks of a bigger railway signalling system. This would only be appealing if they could supply several system integrators, as is the case in other industries. In turn, this would only be possible if standardized and interoperable interfaces are defined. The separation of the building blocks, connected through standard interfaces, also means that the development lifecycle of each block can be managed independently.

The use of COTS equipment leverages the described modularity and interoperability to another level. The possibility to reuse parts and sub-systems not only within the railway industry but also across different industries. This increase in the horizon seen by a company developing this kind of products has a significant impact both in the attractiveness of the activity and in the final cost of the deliverables. Also, from the safety point of view, the much wider installed base positively impacts the RAMS data available, contributing to an increase in overall safety levels.

The most advanced and promising interoperability effort is Eulynx, described below.

2.4 Eulynx

Considering the pressure noticed in the recent years for a more efficient railway network, namely in Europe, several railway infrastructure managers have started initiatives with the aim of promoting interoperability between subcomponents, ultimately leading to the reduction of cost of railway signalling assets.

Although with radically different outcomes, Euro-interlocking and ETCS can be identified as early attempts towards European railway signalling standardisation. Euro-locking aimed at producing the specifications of a common interlocking, usable in all European railway administrations, although it has never reached its purpose. Completely different results had ETCS. After a long period of discussion, the specifications were released and started to be gradually adopted. After its introduction in Europe, its original scope, infrastructure managers all over the world are profiting from the advantages of an interoperable railway signalling sub-system. Although covering only a part of the railway signalling landscape, ETCS can be seen as a success story towards standardisation.

The next step was to consider the possibility of using standard protocols over standard networks to promote modularisation and interoperability. At the beginning, these initiatives were mostly national, focusing on the specific

needs of each network. An example is the NeuPro project (Daffner, et al., 2017), promoted by Deutsche Bahn (DB), started in 2012 with the purpose of promoting standardisation of signalling systems. Later, DB joined several other European infrastructure managers that shared the same goal and Eulynx was formed.

Eulynx is the most well-known initiative in this field, currently composed of 12 railway administrations promoting the adoption of a modular architecture of railway signalling systems. With standardized interfaces between them, each module can be implemented by a different manufacturer and still work seamlessly to build a complete system.

Proving its liveliness Eulynx has already released its Baseline Set 3 Release 2, with Baseline Set 4 scheduled for later this year. The documentation set clearly defines the interface between the interlocking and its typical peripherals, like signals, points or train detection systems. Another significant output of Eulynx is the Reference CCS Architecture (RCA), produced in cooperation with the ERTMS users group (Group ERTMS Users & Eulynx, 2018). This architecture promotes a single modular framework for the command and control of signalling systems, anchored in previously discussed concepts like the use of COTS or the standardization of interfaces.

3 AN APPROACH FOR THE DEVELOPMENT OF SAFE IP PROTOCOLS

The raise of new communication protocols as a consequence of a new generation of IP equipment for railway systems, entails a challenge for system integrators: find an efficient and safe way of implementing those protocols. Thus, next is presented an approach for the development of safety communication protocols, with a special emphasis on the development process, models' creation and properties specification.

3.1 Development Process Overview

The model-based design (Mansour Ahmadian, 19-20 Sept. 2005) proposes a design process where system engineers create the system specification in the form of a model instead of a document. The main goal of this approach is to tackle the problem of misunderstandings/incoherencies between the specification provided by system engineers and the real implementation of systems since the model created during design could be used as a working model for simulation, in order to explain the design in a more simple and dynamic way when compared to (static) specification documents.

The model-based design has emerged for the prototyping of systems. However, with support of more sophisticated features by the model-based tools, it is now possible the use of such tools in the development of complete and complex systems. Currently, some model-based tools (for example: SCADE or Simulink) are able to support all phases of software development process (design, implementation, verification and validation activities), including the more complex ones, as the ones used in the development of safety-critical systems.

The model-based development process allows the creation of complex systems in an efficient way by using mathematical models to design system components and their interactions and then (automatically) generate source code to be integrated in a final target system, as illustrated in Figure 1. The use of a formal language to design systems (mathematical models) provides also the basis to perform mathematical reasoning on them, allowing for example the use of formal methods to ensure system properties.

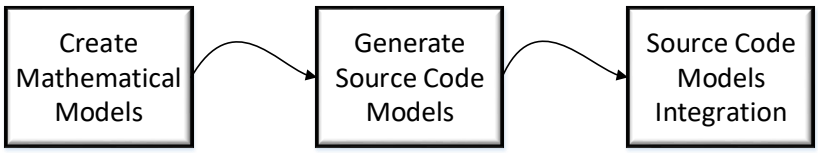

Figure 1 - Model Based Development Process – Implementation

The support for the development of complex system also made the models creation a more complex task, which in some cases requires a level of expertise closer to the one required for the development teams rather than the design teams. Thus, the key advantage of model-based process is no longer the original idea of allowing system engineers to create a model of their system but instead the efficiency of the development process by automating the codification task.

The use of model-based process for the development of safety-critical systems is very common, due to the simulation, testing and formal verification capabilities provided by the modelling tools. These capabilities offer a good support for the heavy verification and validation process that safety-critical systems are required to perform. When the model-based development is applied in the context of safety-critical systems the code generator tool gains even more importance, since we need to ensure that the code generated fully respects the functional behaviour of the designed models. Thus, it is highly recommended the use of a certified code generator in order to be able to apply model-based development for safety-critical systems.

The development process proposed for the creation of safety protocols relies on the model-based development process. This development process is fully compliant with EN50128 (EN50128. Railway applications - Software for railway control and protection, 2011) for SIL4 systems. In fact, it has already been applied in the development of other already certified systems.

3.2 Challenges of Modelling Process

The modelling languages provided by the more sophisticated model-based tools include advanced features suitable for the development of embedded systems. Those features include state machines, data flows, logical operators, temporal operators or higher order functions. All these features are typically available in a textual format but also in a powerful graphical language which provides a good readability of the models.

Regardless of the evolution of modern modelling languages, there is still a considerable gap between the features provided by programming languages and the ones supported by modelling languages. A part of this gap is understandable and not necessarily a disadvantage, since some features provided by programming languages are redundant and other not eligible, due to the formalism demanded by modelling languages. Nevertheless, the gap between programming languages and modelling languages can be in fact a disadvantage, representing an obstacle in the modelling of complex systems. Even though most of the times these obstacles can be overcome with some creativity and expertise.

Despite the power of modelling languages, it is not mandatory that all features of communication protocols need to be modelled. Functions which are not safety relevant or components which are not required for the functional behaviour of the protocol may be added in final target system. This approach could increase the integration effort but could be a solution to some feature that cannot be modelled or to simply have a lighter model, focused on the analysis of the safety aspects.

3.3 Properties Specification Approach

The standard for railway applications concerning communication systems (EN50159. Railway applications - Safety related communication in transmission, 2010) identifies several threats that a transmission system is exposed to, as well as, defence strategies for the identified threats in the attempt of tackling safety and security issues. Messages corruption when message data is violated or message repetition when a message is advertently or inadvertently repeated are just examples of issues that communication protocols need to address.

Communication protocols aiming to be compliant with EN50159 should implement the mentioned defence strategies or use others with the same level of efficiency. In this paper, the details of safety mechanism provided by communication protocols will not be analysed in detail. The focus is on the implementation of protocols and their compliance with designed protocol mechanisms. Nevertheless, the correctness of implementation is performed through the formal verification of system properties, as such, also the defence strategy implemented by communications protocol is (indirectly) verified.

One of the main challenges regarding property specification process is to determine which properties should be proven valid within a system. Should we try to specify all the system behaviour as system properties, or should we focus on some types of properties. The proposed approach intends to focus on protocols safety properties rather than on all system properties. These properties shall be derived from the defence mechanism designed to prevent the threats identified, corresponding to high-level safety requirements for communication protocols systems as illustrated in the examples presented in Table 1.

Threat	Defence Mechanism	Safety Properties
Delay	Timeout mechanism.	1) If no message is received within a given period of time then system shall enter in a fail state.
Repetition	Timestamp mechanism	2) If a message with timestamp not within the current timestamp and the timeout is received then it shall be discarded.
Insertion	Source identifiers	3) If a message from an unexpected source is received then it shall be discarded.
Insertion	Destination identifiers	4) If a message contains a destination identifier different from the expected one then the message shall be discarded.
Corruption	Safety code	5) If a message contains a safety code different than the one calculated then the message shall be discarded.

Table 1 – Examples of Threats, defence mechanisms and properties specification mapping

Even though the implementation of properties could be slightly different from protocol to protocol, since each defines its own implementation of the safety mechanisms with different interfaces and data structures, the specification of properties could be reused. Since the threats and the associated defence mechanisms are almost the same for all the protocols.

As an example, the timeout mechanism present in the majority of communication protocols is typically used to put a system in a fail state when the communication with its partner is broken. However as stated previously, the concrete implementation of safety mechanism can be different. Following the timeout mechanism as an example, the implementation of fail state can be performed in different ways. The fail state of a train detection system could be achieved by setting the status of a track section area as an unknown state or the occupied state (also considered a safe state).

The development process of a safety critical system as the one proposed, encompasses a heavy verification and validation process with several verification and validation activities at all stages of development process (e.g. requirements verification, testing, test coverage). One of these activities may be the formal verification, more precisely, the use of formal methods to ensure system properties (highly recommendable but not mandatory according EN50128 for SIL 4 systems). In the proposed development process to ensure safety related properties the formal verification is included, through one of the most successful formal methods techniques: the model checking technique.

Model Checking is a formal verification technique suitable for assessing the functional properties of systems. Model checking-based methods are among the most successful formal methods in the industrial context, essentially due to their automated nature, since, given a model of a system and a property to verify, model checking answers (automatically) yes or no to the question "Does the model satisfy the property?".

Even though the verification process is automatic, most often human assistance is required to overcome a few obstacles. Arguably, the biggest of these obstacles is the state explosion problem (Valmari, 1998). This problem prevents the verification process to end (or at least, to end in an acceptable period of time) due to the huge size of models state space, which requires then, a huge amount of time to perform the exhaustive search required by model checking technique.

The evolution of model checking technique is very dependent on the development of techniques that are capable of tackling the state explosion problem. Therefore, a big effort to find these techniques has been made in the model checking related research field (Edmund M. Clarke, 2012). The model-based tools include some of the most advanced model checking algorithms. Nevertheless, they were not able to solve the state explosion problem entirely. Thus, it is important to have in mind that building simple models or specify accurate properties could be

the key for a successful formal verification activity. Removing non-safety functions from your model could be a good decision if the focus is on the safety properties and there is the need to perform a model simplification.

The property specification process, as well as the formal verification of those properties can be very time-consuming tasks due to the challenges already mentioned. Thus, the presented approach where only safety properties were considered, provides in our opinion an interesting cost-effective solution.

4 CASE STUDY – FRAUSCHER SAFE ETHERNET PROTOCOL

The implementation of the Frauscher Safe Ethernet (FSE) is first case study used to demonstrate the feasibility of the approach presented for the development of safe communication protocols. FSE is a communication protocol designed to deal with safety information, implementing several of the common safety mechanisms concerning communication protocols. In addition, it is already certified, and so well framed regarding the railway standards. In our opinion, FSE fulfils all the requirements to serve as the basis to validate the proposed development approach.

4.1 Frauscher Safe Ethernet Protocol

The Frauscher train detection system is based on the axle counting technology, where the axles of vehicles are counted in when a vehicle is entering a predefined area and counted out when the train is leaving, meaning that a given area is clear of trains if there are no axles counted for this area.

The Frauscher Safe Ethernet (Sommergruber, 2015) is a communication protocol to provide an interface between train detection system and higher-level signalling systems like interlocking systems. FSE is a freely available protocol developed by Frauscher to provide a communication interface with their train detection system fulfilling all the safety requirements demanded for the higher integrity level (SIL 4) according to the applicable railway standards. The FSE is a protocol certified according EN 50159 for Category 2, which means that it contains protective measures to run safely in network environments where the number of equipment is not limited and the characteristic of transmission system may be unknown but where the risk of unauthorized accesses is negligible.

Currently, FSE is suitable for use in the majority of railway infrastructures as they have their own network (closed network), thus having the characteristics defined for Category 2 according EN 50159. However, with the demand to reduce infrastructure costs, the need of a higher integration between railway systems and external systems and the consolidation of protocols regarding security protective measures (cryptographic techniques) this situation may change in near future.

The transition from electrical interfaces to communication interfaces allowed a wider range of data to be collected from trackside equipment systems, since additional information has almost no cost for communication interfaces. The Frauscher train detection system proves also this statement, since FSE provides several different information regarding train detection system. This information includes the common data concerning the presence of vehicle within an area, to less common information like the diameter of train wheels.

4.2 A model of Frauscher Safe Ethernet Protocol

The amount of data included in the protocol and the possible configurations of message structure, with data being only included in a specific application if required, raises a challenge for the creation of a model due to the variability of data length. In addition, the FSE protocol implements some of the common safety mechanisms like the use of source and destination identifiers to prevent the possibility of unidentified partners enter in the communication loop or timeout mechanism to detect when a communication is interrupted.

Despite the mentioned challenges, it was possible to model almost entirely the FSE protocol, thanks to the powerful features provided by model-based tools in combination with some expertise and creativity. Only one function was left out from the created model, the one related with socket management. Since this function is not relevant for the protocol behaviour, and even less relevant for the analysis of the safety aspects. Furthermore, some of the socket management features are hard to model due to the lack of support by model-based tools.

The created model has successfully been integrated in a final target system, and it is part of a solution working in a real scenario. In this scenario, an IP interface is performed with Frauscher train detection system, namely with

Frauscher Advance Counter (FAdC) product in order to obtain the safe information regarding the presence of trains within track section areas.

4.3 Formal Verification of Frauscher Safe Ethernet Protocol

The proposed property specification strategy aims to verify whether the model of FSE communication protocol contains the safety properties derived from safety protective measures. The main idea behind the proposed strategy is that communication protocols share several safety protective measures and so, the creation of generic safety properties is possible and could be reused for each protocol implementation with some adaptations. In order to prove this concept, the mapping of high-level safety properties (see chapter 3.3) to the safety properties to be verified in FSE protocol is illustrated in Table 2.

The properties specified are no more than safety requirements, where the generic properties correspond to high-level safety requirements and the FSE properties correspond to FSE safety requirements. Thus, the specified FSE safety properties were driven/adapted from FSE functional specification, more precisely, from FSE safety requirements. Please note, that the mentioned adaptation from FSE safety requirements is only the rewritten of those requirements in safety-oriented format, more aligned with the formalism required.

High-level Safety Properties	FSE Safety Properties
1) If no message is received within a given period of time then system shall enter in a fail state.	If no message is received within a given period of time then all statues shall be set with value 0.
2) If a message with timestamp not within the current timestamp and the timeout is received then it shall be discarded.	If the current own timestamp minus the RX timestamp, is smaller than the timeout then the message must be discarded.
	If the TX timestamp of the current message minus the TX timestamp for the last message is not smaller than the timeout and greater than 0 then message must be discarded.
3) If a message from an unexpected source identifier is received then it shall be discarded.	If the configured communication partner address does not match the source address of message then message shall be discarded.
4) If a message contains a destination identifier different from the expected identifier then the message shall be discarded.	If the receiver's own address and the destination address of the message does not match then message shall be discarded.
5) If a message contains a safety code different than the one calculated then the message shall be discarded.	If a received message contains a CRC code different than the one calculated then the message shall be discarded.
	If a received message contains a CRCi code different than the one calculated then the message shall be discarded.

Table 2 - Mapping of high-level safety properties and FSE safety properties

The first high-level property stated that the system shall enter in a fail state if no valid message is received within a given time, the mapping of this property to the FSE properties is simple, requiring only the definition of how FSE implements the fail state. The implementation of FSE for the fail state is to set all statuses to value 0. In order to understand if this approach is valid or not, it would require the analysis of the expected statuses. This kind of analysis is not within the goals of this paper. The focus is to prove that communication protocol is well implemented concerning the defined safety mechanisms.

Concerning the second high-level safety property two different FSE properties were driven. These properties state that a message with a timestamp not within the correct time frame shall be discarded. Since the FSE protocol uses two different timestamps one for the receiver and another one for the sender, both timestamps need to be verified regarding the expected time frame. Thus, two properties need to be proved (one for each timestamp) in order to prove the high-level property.

Regarding third and fourth safety properties, both refer to the verification of sender and destination partners. The third property checks that messages received from an unexpected partner should be discarded, while the fourth verifies that a message received with a destination identifier different from the configured own address shall be discarded. The mapping of these properties to the FSE is almost straightforward, since both source and destination identifiers are part of protocol configuration. Thus, a message shall be discarded if one of these identifiers do not match with ones received in the message.

The fifth property states that safety code calculated in the origin and destination partners must match otherwise a message is not valid. This property gives origin to two different properties, once the FSE protocol defines two different safety codes to be calculated for each message, both using Cyclic Redundancy Check (CRC) method but one using inverted data to perform the calculation, described as CRCi.

5 CONCLUSION

The presented approach for the development of safe communication protocols has been validated by the successful implementation of FSE using this approach. Proving the power of modelling process, as well as the viability of the model-based development process.

Arguably, the main advantages of this approach are the efficiency provided by model-based development and the correctness obtained with formal verification process. Whereas, the main challenges are the execution of formal verification due to the obstacles like state explosion and the modelling of safe protocols due to the expertise required.

Concerning the properties specification process, it would be interesting to have more protocols being implemented following this approach, in order to understand better the level of reuse provided by the properties specified for the FSE protocol. In addition, the high-level properties specified could be also a guide to find weaknesses in the new protocols even if the focus is on implementation rather than on the design of protocols.

6 REFERENCES

Daffner, P., Eisenbrandt, H. & Beck, T., 2017. Pilot general contractor model for the Heidingsfeld electronic interlocking project. *Signal+Draht.*

Edmund M. Clarke, W. K. M. N. P. Z., 2012. Model Checking and the State Explosion Problem. Em: *Tools for Practical Software Verification..* Berlim: Springer, Berlin, Heidelberg, pp. 1-30.

EN50128. Railway applications - Software for railway control and protection (2011) CENELEC, European Committee for Electrotechnical Standardization.

EN50159. Railway applications - Safety related communication in transmission (2010) CENELEC, European Committee for Electrotechnical Standardization.

Group ERTMS Users & Eulynx, 2018. *White paper reference CCS architecture based on ERTMS.* s.l., s.n.

Leach, M., 1991. *Railway Control Systems.* London: A & C Black.

Mansour Ahmadian, Z. (. N. N. K., 19-20 Sept. 2005. *MODEL BASED DESIGN AND SDR.* London, UK, IET.

Sommergruber, M., 2015. *Benefits of modern train detection systems.* Melbourne, Victoria, Australia, AusRAIL PLUS.

Valmari, A., 1998. The state explosion problem. Em: *Lectures on Petri Nets I: Basic Models.* . Berlim: Springer, Berlin, Heidelberg, pp. 429-528.