DISTRIBUTED RAILWAY SIGNALLING ARCHITECTURES WITH OBJECT CONTROLLERS

Florian Einböck, Product Manager FAdC® and EULYNX Object Controller, Frauscher Sensor Technology
Manuel Forstner, System Architect, Frauscher Sensor Technology
Stefan Neudorfer, Cyber Security Expert, Frauscher Sensor Technology

SUMMARY

With the increasing digitalisation of the railway industry, new demands are being placed on railway architectures. Since railway signalling applications and connectivity concepts have different life cycle requirements, a clear distinction between safety and security must be established.

A safety system is expected to be particularly durable and low maintenance, whereas a security concept must react in an agile and dynamic way to new requirements and threats. Object controllers open up the possibility of meeting these requirements and enable data and information to be transmitted via EN 50159 cat 3 networks to both interlockings and customer diagnostic systems. Furthermore, object controller features are key to success with regards to distributed architectures in railway signalling. Through distributed architectures and the implementation of the safety function in the object controller, it is possible to ensure the real-time capability of safety-relevant applications.

1 INTRODUCTION

The immense expansion of passenger and freight traffic urges railways to accelerate modernisation. Improving the performance of train detection systems by means of intelligent object controller solutions in conjunction with digital interlockings marks an important cornerstone of appropriate strategies.

To enhance the infrastructure for related projects, several initiatives have been introduced during the past decades, such as European Train Control System (ETCS), Communications Based Train Control (CBTC) or Digital Automatic Coupling (DAC). The common goal of these is to transform railways into a more digital environment by promoting the use of software-based solutions and appropriate communication networks. This not only saves hardware components, space, and resources, but also makes railways more cost efficient and boosts their overall capacities. However, as the position of components which process, communicate and transfer sensitive data within a system is changing, new possibilities are arising along with new challenges.

Against that background, this paper focusses on the aspects of harnessing a more digitalised infrastructure in vital railway applications, such as train detection systems, whilst considering safety requirements and new security concepts that must come with the use of new technologies, and the consequences of these for future-proofing components of highly innovative railway applications.

2 SAFETY AND SECURITY

The foundation that underpins increasingly digitalised railway applications is reliable connectivity, through which individual components of respective systems exchange vital and non-vital information. For instance, these range from track vacancy detection information to extensive diagnostic data. Considering the range of information, these networks must meet the latest requirements in terms of safety and security.

In the history of the railway industry, concepts for safety and security have already existed for a long period of time. However, introducing more software-based solutions and digital networks to realise applications such as train detection requires a closer inspection of these two terms. The principle of applying safety and security frameworks is far from being new, but as the subjects that they're handling are increasingly digitalising, new aspects must be considered. That said, the difference between railway related safety and security systems can be identified via their field of focus.

Safety is focusing on operational aspects in train operations, while security, with its roots in IT architecture, is becoming an increasingly established term in the context of using software-based solutions, including open communication networks. To create future-proof solutions, a mutual relationship between these two concepts must be taken into account: safety functions must be protected by security functions, while security functions must not compromise the safety functions. To explore the effect of increasing digitalisation on existing safety and security concepts as well as future initiatives, the following chapter aims to investigate their individual meaning and highlights the most important aspects when it comes to combining safety and security in future-proof railway solutions, using train detection as an example.

2.1 Safety

Railway-related safety concepts are focusing mainly on operational aspects. Their purpose is to ensure and protect operational safety, which involves defining frameworks for the development, installation, and use of signalling technology, such as axle counters, for instance. Significant aspects such as reliability, transparency, precision, and a long service life of up to 25 years and more are the basic requirements that must be demonstrably fulfilled by the components in use.

Norms and standards, according to which safety concepts are developed, can differ from country to country, but are quite similar over wide areas of Europe for example. The initiatives mentioned in chapter 1 are contributing towards a homogenisation of this framework and support the application of evolving security concepts in the future, as we will explore in the following chapter. To ensure safety-relevant guidelines are considered at all stages of a product lifecycle, well-known RAMS (Reliability, Availability, Maintainability, Safety) concepts are applied to monitor its ongoing compliance with corresponding regulations during development and to ensure standardised processes are considered throughout operation and maintenance. As the latter always means intervention in operation, appropriate guidelines have been established to ensure that the safety-relevant characteristics of a maintained component must never be changed or affected during maintenance works without considering their safety-relevance.

In case a major adaption of a system component needs to be performed, for example due to severe damage, the resulting changes must be documented, and the system must be tested intensively before it can be placed back into operation. Considering the nature of software-based solutions, which can receive regular updates for example, these requirements must be considered in the development and rollout of new software versions in the field. Applicable regulations are defined in the EN 50128, which was developed to accompany the increasing use of software in safety relevant systems. Here, a clear roadmap can be found that describes the detailed requirements for each stage in a development process – from evaluating requirements, through setting up a safety concept, identifying and locating safety functionalities to final testing, validation, and acceptance. This process must be followed rigorously, especially when it comes to maintenance, so that it is clearly defined at which stage of the process the relevant activities must be relaunched. The principle of transparency precisely defines roles and distributes responsibilities amongst various experts involved in these activities to guarantee independence and quality. The sheer complexity and manpower required to develop and maintain software-based solutions in safety-relevant systems turns out as labour-intensive in light of this background. However, since vital applications such as train detection are handled by such systems, it is absolutely necessary to consider these regulations.

On the other hand, this complexity builds a contrast for both the potential and requirement of software-based solutions when it comes to adapting to a dynamic environment. On the one hand, new possibilities and features are constantly arising which can increase a railway system's performance when implemented via constant updates. On the other hand, by transferring these applications into a more digital environment, they are increasingly opposed to external threats – a factor that is potentiated by the use of open communication networks. While communication between safety-relevant components was realised for example via IO modules up to now, new concepts allow the use of fully digital and open networks to increase speed and volume of information-exchange. However, this also opens the gates for potential new threats that are relevant for safety-concepts, but must be covered by security architectures, as we will see in the next chapter.

2.2 Security

Security-concepts consider all kinds of potential external risks and threats that might affect an actively operating system – such as a train detection system used in a railway network. There are two main factors to be considered in these concepts, namely threats and vulnerabilities. The latter can be caused for example by flaws during the development stage. Threats are caused by external protagonists, who are looking for access points, such as these vulnerabilities, and use them to enter and manipulate the system. The IEC 62443 standard defines four security levels, at which protection against certain threats must be achieved:

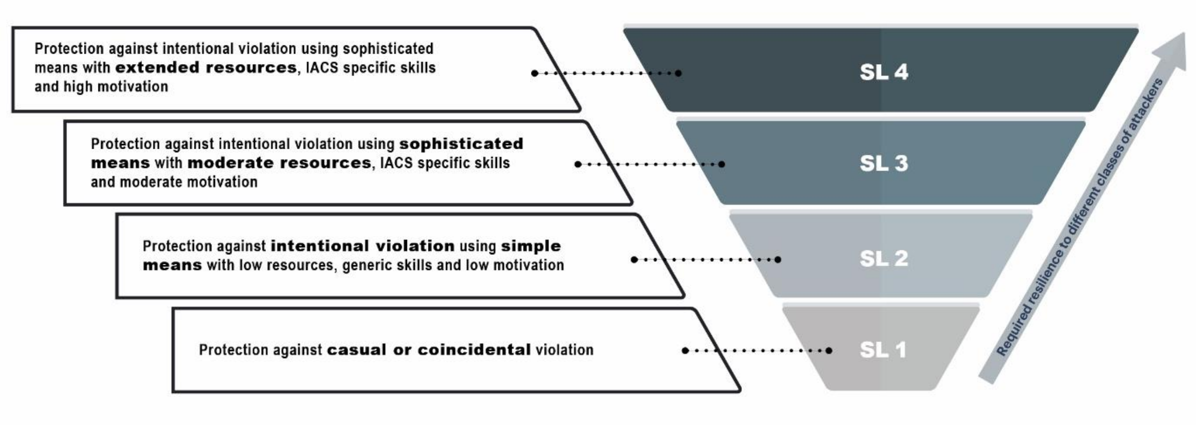
Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation
Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
Protection against intentional violation using simple means with low resources, generic skills and low motivation
Protection against casual or coincidental violation
SL 4
SL 3
SL 2
SL 1
Required resilience to different classes of attackers

Figure 1: Security Levels according to IEC 62443

Thus, the measures on each security level must adapt to the rising potential behind the threats. Avoiding vulnerabilities and maintaining fail-safe operation serves as an important cornerstone in increasing a system's resilience against such influences. That said, the relevance of safety-concepts when developing software-based solutions for vital railway applications, such as train detection, becomes even more obvious. In the same spirit, security must take on prescribed roles in the process described in chapter 2.1 to cover relevant activities throughout all development stages in order to avoid vulnerabilities in the first place. However, solid security concepts are equally, if not more, important during operation. When utilising open networks for active data transfer between components in software-based solutions, further access points for potential threats arise in the field.

To empower the use of digital networks, applicable components must be added to safety-relevant systems. Some of these are components off the shelf (COTS), which have a huge benefit in terms of speed, as there is no need to develop them separately. By being added to the system, they have a high relevance for security frameworks, as they form potential access points and must therefore be considered in appropriate concepts to monitor and manage them.

The increasing use of open networks is another aspect that adds to the requirements in terms of security concepts for safety relevant systems. Harnessing the possibilities of highly efficient transfer of information and data, single components within a system can take over more responsibilities and functions, which ultimately leads to more decentralised architectures. Although the use of non-isolated communication channels reduces efforts and costs while increasing the speed of implementation and data transfer, it also brings more potential of being accessed by external protagonists who are rapidly adopting to new possibilities, using highly specialised knowledge to exploit the latest security gaps as they occur. That said, security concepts must not only follow strict protocols to apply to pre-defined safety-guidelines, but they must also be able to adapt to a very dynamic environment in order to protect vital systems against potential risks that are changing day by day.

Thus, applying security concepts on increasingly digitalised systems for future-proof, safety-relevant railway applications mean that there must be a certain space for dynamic updates and changes to increase resilience against rapidly changing risks. Initiatives, such as the European Cyber Resilience Act are currently setting first steps towards defining a framework for relevant processes. Furthermore, standards such as the above-mentioned IEC 62443 are now providing a guideline to maximise cyber security of software-based systems. However, in light of the increasing digitalisation and a growing shift towards decentralised architectures, existing regulations that describe the process and standards for safety-relevant railway systems must potentially be reviewed to a certain extent – or in some cases, it will be necessary to define new norms, as certain aspects of using software-based, digital solutions in railway operations are not covered by known regulations at the moment. The challenge that comes with that is clear: Due to the highly dynamic nature of the environment to which these concepts must be applied, it is much more difficult to define fixed norms and standards to which these systems are oriented.

2.3 Safety and Security: Combining Two Universes for Future-proof Railway Applications

While safety concepts are there to ensure consistent operational integrity during all moments of a system and its component's lifecycle, security concepts exist to protect the system within which these components are operating against vulnerabilities and external threats. When it comes to the use of digital solutions for railway applications, an intelligent combination of both is crucial.

The contrast is within the purpose of both conceptual worlds. While safety concepts are meant to create long-lasting frameworks for products with a lifecycle of several decades, security concepts are focusing on the more dynamic world that arises mainly by the use of digital networks. More dynamic security concepts will be required in the future, which can cause contradictions to the firstly described frameworks of safety concepts.

That said, the intersection of these two concepts defines the field of operation for future-proof, digital solutions in vital railway operations: On the one hand, these solutions need to imply long-term concepts that ensure fail-safe operations. On the other hand, they need to be flexible enough to be adaptable according to the ever-changing range of possibilities and threats of a digitalised environment.

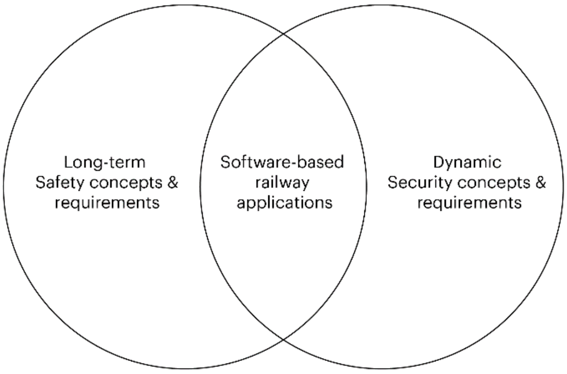
Long-term
Safety concepts & requirements
Software-based railway applications
Dynamic
Security concepts & requirements

Figure 2: Intersections of safety and security concepts

Considering existing norms and standards for cyber security, TS 50701 integrates IEC 62243 into the railway sector by linking it to the V-model (EN 50126). Essential points of synchronisation that are needed to achieve coordination among security activities and all stakeholders, include: system engineering, safety, RAM, V&V, and T&C activities:

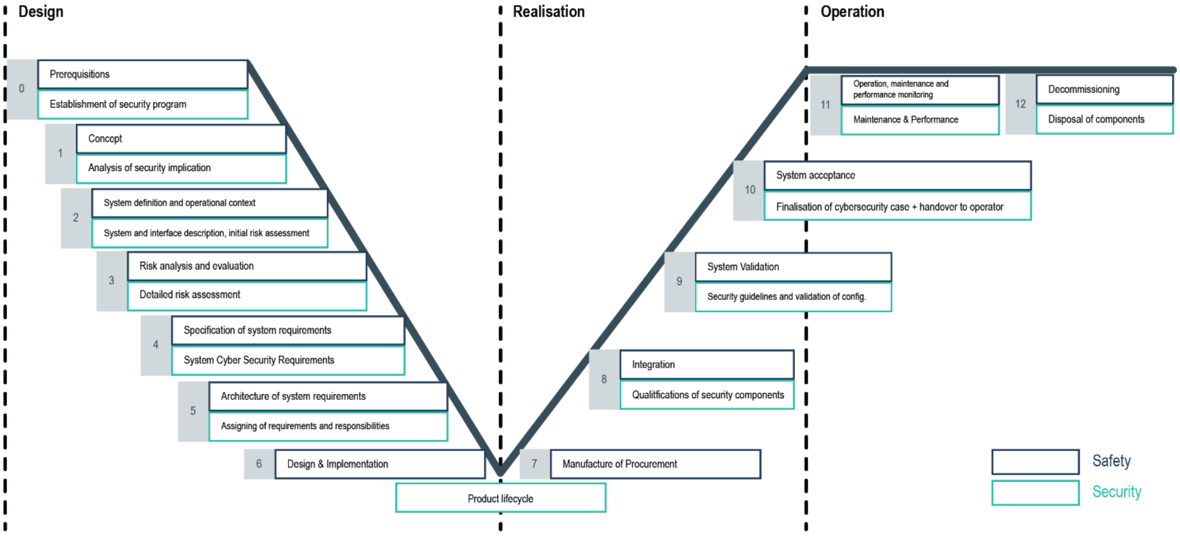
Design
Realisation
Operation
0
Prerequisitions
Establishment of security program
1
Concept
Analysis of security implication
2
System definition and operational context
System and interface description, initial risk assessment
3
Risk analysis and evaluation
Detailed risk assessment
4
Specification of system requirements
System Cyber Security Requirements
5
Architecture of system requirements
Assigning of requirements and responsibilities
6
Design & Implementation
Product lifecycle
7
Manufacture of Procurement
8
Integration
Qualitfications of security components
9
System Validation
Security guidelines and validation of config.
10
System acceptance
Finalisation of cybersecurity case + handover to operator
11
Operation, maintenance and performance monitoring
Maintenance & Performance
12
Decommissioning
Disposal of components
Safety
Security

Figure 3: Safety and Security Process (according to SIST-TS CLC/TS 50701:2021)

Considering the complexity of a combination of safety-and security-concepts, this model suggests a practicable approach to manage this. Facing the fact that while up to now, hardware-based systems have been status quo in the railway industry, initiatives such as the ones that were mentioned in the introduction of this paper, accelerate the establishment of a digital system, such as digital interlockings and their relevant communication networks. Also, in terms of diagnostics and maintenance, digitalisation is changing the way in which railway networks are performing. Thus, it is necessary to unite established safety standards in the railway industry with new security concepts or, even to enrich them. The mere coexistence of software-based solutions and proven systems based on relays and cabling will not meet the growing requirements of an increasingly digitalised railway.

2.4 Framework for Future-proof Railway Operations

In light of the developments described in chapter 2, a framework is required to use cutting edge technologies for future-proofing railway operations. A common standard for train control is being established, namely the European Train Control System (ETCS). To standardise the digital connection between interlockings and field elements in this system, an initiative named EULYNX was founded. The goal of this initiative is to establish standards for interfaces used in interlockings and between subsystems to ensure that different components will communicate seamlessly, irrespective of their origin. By establishing such a standard, it should be possible to firstly harmonise the ever-growing number of solutions and ensure they are communicating in the same language. As a result, full flexibility in choosing components to be combined within a system is enabled. Additionally, significant time and cost savings are achieved, as efforts for coordination of interoperability are reduced to a minimum. As an additional benefit, the overall saving in terms of cabling and additional hardware can be increased.

The latter is especially based on the growing use of open networks. In that context, the Comité Européen de Normalisation Electrotechnique (CENELEC) defines requirements towards railway applications in its EN 50159. This norm is the central document that collects requirements for safety relevant electronic systems that are used for digital data transfer. It describes three categories and explains the prerequisites for using them:

- Transmission system that is under the control of the designer and remains unchangeable during the lifecycle (category 1), or
- Transmission system that is partially unknown and also not immutable, but where unauthorised access can be excluded (category 2), or
- Transmission system not under the designer's control and for which unauthorized access must also be considered (category 3)

Formerly, railway systems used mainly category 1 networks. In the past decade, an increased number of systems were installed that also used category 2 networks. With a massive increase of digital solutions, the use of category 3 networks has gained relevance.

The requirements based on EULYNX and the additional challenges introduced by the use of category 3 networks form a framework when it comes to the development of future-proof digital interlockings and other safety-relevant systems as well as their corresponding field elements. Concerning the latter, object controllers experience an increasing relevance as they form the interface between trackside equipment and the interlocking. Transmitting data and information, vital and non-vital, creates a range of new requirements to be considered when developing them.

3 OBJECT CONTROLLER CONCEPTS TO EMPOWER DISTRIBUTED ARCHITECTURES

Object controllers are well-known components of railway systems. In essence, they function as an interface between trackside assets and interlocking computers, by giving commands and receiving messages from the trackside assets such as points and axle counters. In the course of digitalisation, both new challenges and opportunities are arising whereby object controllers become the answer to the modern requirements of operators considering both safety and security.

However, the role of object controllers has changed due to connectivity requirements, and they are becoming a key element in modern, distributed railway architectures. Consequently, object controllers are helping to increase system efficiency and its more cost-effective realisation, whilst empowering preventive maintenance by enabling remote access to diagnostic data. At the same time, they also require the increased integration of additional functions, such as alarms and other measures for better cyber security.

	Existing OC	Modern OC
Location of OC	Interlocking room	Cabinet can be next to rail
Distance of OC to trackside asset	Up to 10 km	Close to the trackside asset
Communication to interlocking	Proprietary protocols via proprietary electrical connections (card slots)	Redundant IP based protocols via ethernet or wireless
Procurement process	Everything from a single source	Independent suppliers possible
life cycle	Tightly coupled with interlocking	Decoupled from interlocking (separation of concerns)
Scalability and extendibility	Additional hardware and cabling	On interlocking side only software configuration change No cabling reasoned by network
Diagnostics	Individual (proprietary) diagnostic concept	Designed to access and evaluate diagnostic data remotely
Maintenance (SW & configuration update)	Local roll out	Centralised (remote) roll out possible
Network security	Designed for closed network communication	Designed for open network communication
Safety assessment	Need for overall assessment very likely	Separate assessments for interlocking and OC (separation of concerns)

Being equipped with this logic, object controllers are taking on the responsibility to fulfil tasks that were previously assigned to interlocking computers. They are receiving and processing information and then command and control the respective trackside assets in real time to meet the requirements of safety systems. In turn, this allows for highly efficient, distributed architectures to be established. Taking all things into consideration, the main goal when establishing future-proof systems on that base is a safe connection between an object controller and field elements. According to the safety-relevant nature of these field elements, this connection has to be able to transfer data within very precise timing constrains. In other words, control, monitoring and evaluation must be carried out safely and in real time.

From the object controller to the interlocking, data and information can be subsequently transferred via open networks. However, by adding open cat. 3 networks, additional cyber security concepts are required, as described in chapter 2.2. Thus, operational as well as diagnostic data is now available to a broad range of receivers, even by means of remote access. In light of what was described in the aforementioned part of this paper, this also means that now, safety relevant functions are moving from the interlocking into a more distributed structure along the track, while security requirements are increasing due to the open nature of the communication networks in use. Thus, ways of securing the communication must be installed and possibilities to implement regular updates must be given. This requires a continuous process from the supplier to the operator which enables to provide update versions via a secure channel.

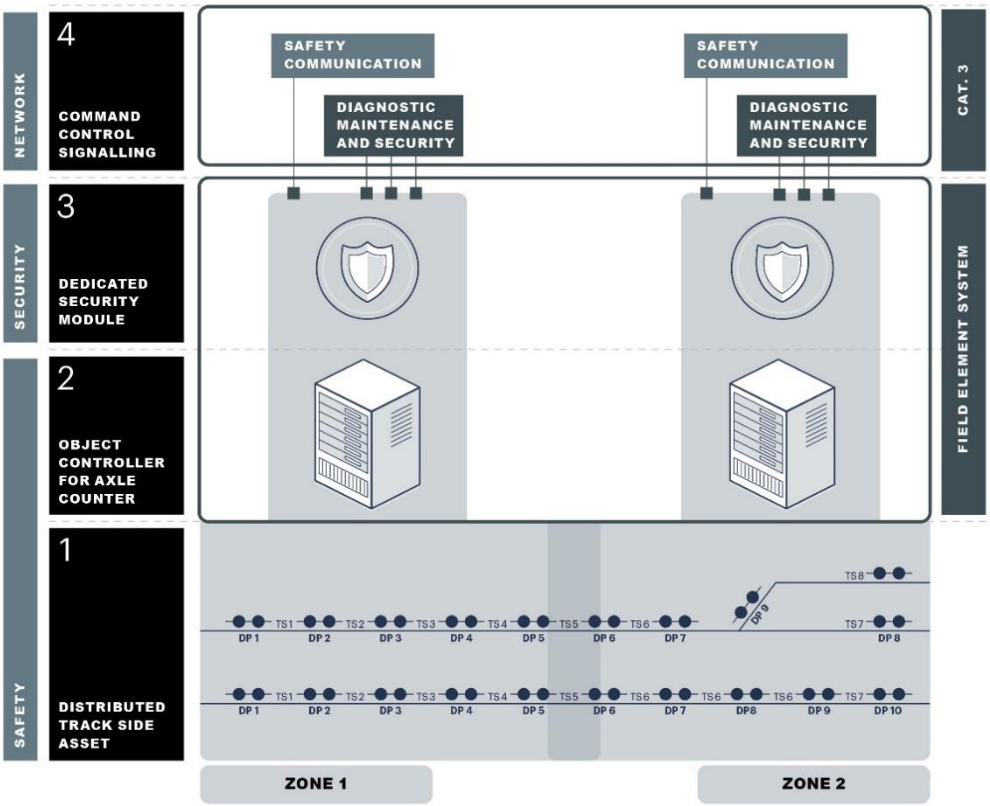
NETWORK
4
COMMAND CONTROL SIGNALLING
SAFETY COMMUNICATION
DIAGNOSTIC MAINTENANCE AND SECURITY
SAFETY COMMUNICATION
DIAGNOSTIC MAINTENANCE AND SECURITY
CAT. 3
SECURITY
3
DEDICATED SECURITY MODULE
FIELD ELEMENT SYSTEM
2
OBJECT CONTROLLER FOR AXLE COUNTER
SAFETY
1
DISTRIBUTED TRACK SIDE ASSET
TS1
TS2
TS3
TS4
TS5
TS6
TS7
TS8
DP 1
DP 2
DP 3
DP 4
DP 5
DP 6
DP 7
DP 8
DP 9
DP 10
ZONE 1
ZONE 2

Figure 4: Distributed architecture with modern object controller

However, within the track environment itself, a distributed architecture which uses object controllers in field only requires the installation of a compact device that can control several components at the same time. These units are directly connected to the central interlocking.

One of the main advantages of this approach is that extensions of railway signalling infrastructure are comparatively easy to realise as only the relevant object controllers need to be added. In this way, also outdated systems can be integrated into modern architectures, as for example, it is possible to combine parallel interfaces, e.g., via input/output card to the existing infrastructure and serial Ethernet interfaces to the interlocking. In total, the implementation of distributed architectures using intelligent object controllers results in savings of resources and an increase in the railway networks efficiency, while empowering scalability and supporting preventive maintenance strategies.

4 CONCLUSION

The railway industry is facing a rapidly growing requirement to increase efficiency while reducing costs. Latest possibilities of harnessing the potential of digital solutions empower the industry to respond to the challenges that come with this. While software-based solutions have been established in railway applications for a long time, new possibilities to use open communication networks and build decentralised architectures introduce the need to rethink certain aspects of safety and security concepts.

Vital application sectors, such as signalling, can increase their performance according to the latest capacity requirements – but their safety critical nature urges for security concepts that combine the framework of established norms and standards with the high dynamics of an increasingly digitalised environment.

As described in this paper, an intelligent framework to combine safety and security concepts is required to overcome this gap and harness the full potential of cutting-edge solutions. While relevant initiatives, such as EULYNX, are already setting first steps towards this direction, there will be further aspects to be considered and discussed, once the distribution of intelligent field equipment, smart object controllers and digital interlockings is in full progress.

5 REFERENCES

1. CENELEC, CLC/TS 50701:2021, 2021
2. CENELEC, EN 50126-1, 2017
3. CENELEC, EN 50128:2011, 2011
4. CENELEC, EN 50159:2010, 2010
5. EN IEC 62443-3-3, 2020
6. Lars Schnieder, Safety und Security in der Zulassung von Bahnanwendungen, EI 06/2016
7. UNIFE, UNIFE Vision on Cyber-Security in Railways, 2020
8. UNIFE, UNIFE Vision Paper on Digitalisation, 2020