Working Group CYSIS

IT/ OT-Security for
Internet of Railway Things (IoRT)

Supported by:

Publisher:

WG CYSIS
UG IT Security IoRT

18.01.2021

Content

1 Management Summary

The increasing use of IP-based objects, services and protocols ("things") as well as communication networks opens up completely new possibilities for the rail sector within the framework of the digitalisation strategy to increase capacities while simultaneously optimizing economic efficiency and profitability as well as increasing customer benefits. At DB Netz, for example, the current more than 3,000 interlockings, which on the one hand are based on very different technologies (from mechanical to electronic/digital) and on the other operate as completely isolated and closed systems, are being placed on a uniform architectural basis as part of the NeuPro architecture (digital interlockings [1]).

A part of these services is the IoT (Internet of Things), i.e., sensors and actuators, which generate various data used to improve railroad efficiency and operations. The term IoT implies a variety of objects (sensors, actuators), technologies and protocols that exchange data over communication networks. The term IoRT (Internet of Railway Things) refers to objects deployed in the railroad environment (on the track, in the train, etc.).

The use of IoT and IoRT, and in particular the networking of a large number of objects, gives rise to new threats, hazards and risks with regard to IT security that must be considered comprehensively and in detail. Consequently, in addition to questions of operational safety, which are traditionally considered in railroad operations, questions of security (detection and defense against cyber threats) must also be considered.

In this white paper, a description of a reference model for IoT is given and then different use cases for IoT in the railroad context are analysed. In the first part, these are standard IoT use cases for optimizing passenger distribution, the traveller experience, and in the area of violence prevention. The second part of the white paper describes two use cases in railway command and control systems that demonstrate the employment of rail-specific actuators and sensors. These are condition-based and predictive maintenance as well as local situation detection in operational rail operations (e.g., reporting of foreign objects in the track area).

Based on these partly very different use cases, threat scenarios for IoRT are considered based on BSI ICS threats, and suitable solution approaches are outlined and described. In this connection, the NeuPro architecture, synchronized with EULYNX in Europe, which was developed as part of the digitalisation of interlocking technology and results from the "HASELNUSS" [2] research project funded by the German Federal Ministry of Education and Research (BMBF), and enabling IT security functions into networked command and control systems, are both included.

2 Introduction

The term "Internet of Things" or "IoT" first appeared in 1999 and at that time described a future world in which all physical objects were equipped with so-called RFID (radio-frequency identification) tags so that they could be in real time and data queries could be initiated via the Internet. Since that time, the scope of meaning has nonetheless expanded, and the term IoT now encompasses a wide variety of objects, technologies, and protocols that, contrary to the term "Internet," do not per se have to be connected or accessible via the Internet. In particular, embedded systems, most of which are equipped with a number of sensors, have made their way into everyday life. IoT now cherishes as its vision a linkage of everyday electronic devices and sensors that share data and become part of a digital infrastructure. This creates an image of the real world in the form of data that can be used to efficiently process a wide range of problems in an automated manner.

By linking local devices with a unique identity, a usable connection is created between the physical world of things and the virtual world of data [3]. This takes account of a key feature of digitalisation - namely the exponential increase in the volume of data on the one hand and the applications or algorithms and computing power required for the business-relevant processing of this data on the other. The business relevance of the data or the processed data ranges from increased transparency, which is required to increase security or optimize processes, to prognostic procedures, which form the basis for increasing effectiveness, to various types of automation, whether by means of rule-based expert systems or by means of neural networks, which form the basis for increasing efficiency and minimizing risk.

The increased importance of IoT made it necessary to create a corresponding frame of reference. This was done in a comprehensive form, for example, by the IoT World Forum [4] [5]. In view of the already existing multitude of networked sensors and actuators as well as data-processing components in the railroad infrastructure, it makes sense to transfer the concepts developed for IoT to the railroad sector. For this purpose, a reference model for an "Internet of Railway Things" or "IoRT" is described based on this reference framework, whereby IoRT is understood to a certain extent as a subset of IoT - namely as IoT objects and technologies optimized for use in the rail environment to enable the corresponding safety objectives in rail operations. Through predictive maintenance of operational components, these services can lead to the reduction of unexpected disruptions in operations; IoRT can also be used to increase the range of accompanying products and services as well as the level of customer satisfaction through greater personalization of offerings.

In order to enable the desired increase in performance in the long term and to minimize the possible security threats to the objects caused by networking and to adequately protect the downstream systems of IT (information technology) and OT (operational technology), it is necessary to investigate the issue of IT security of IoRT systems. To this end, the "Internet of Railway Things" project of the "Cybersecurity for Safety Critical Infrastructures" working group (WG CYSIS) has intensively addressed the areas of application of IoRT and the resulting hazards and protective measures. For this purpose, security objectives are defined that lead to requirements for IoRT systems. Another reason for this white paper is the steadily increasing number of cyber attacks - also in the field of IoT. Consequently, it can be expected that rail infrastructures will also be affected by this in the future. Interventions in the rail system must be prevented or measures must be taken to minimize the effects in the event of an attack to maintain smooth and secure rail operations.

This white paper is the result of the security considerations and sets out general security requirements for the use of IIoT ("Industrial Internet of Things") and IoRT in specific areas of rail infrastructure. The different tasks depending on the operational or security relevance and the resulting requirements for them as well as conclusions on IT security are addressed. At the end, the general structure for systems extended by IoRT-related services is first defined in a reference model. Subsequently, two concrete representative application areas for which existing system architectures have been supplemented by components for the use of IoRT, so-called use cases, are examined in more detail regarding the implications for IT security. The security requirements identified in this process are then abstracted from the system architecture and summarized as general security requirements.

3 General structure IoT/IoRT

3.1 Reference model for IoT

In IoT systems, data from a wide variety of objects, each of which is assigned a unique identity, is generated, and processed in different, business-relevant ways by corresponding applications or algorithms. The location of both the data-generating objects and the data-processing units is not subject to any model-related restrictions and can be selected depending on other requirements; for example, data processing can take place directly at the location of data generation in the case of real-time requirements. The data streams are therefore multi-directional. The IoT reference model proposed in the IoT World Forum takes this into account (see Figure 1); it comprises seven layers, each assigned with a different function, together forming a complete IoT system.

The **first layer** is formed by the physical devices and controllers that control multiple devices - these are the actual Things. The IoT "Things" in this first layer perform the following functions: they generate data, they convert signals from analog to digital representation, and they can be queried or controlled over a network. The "things" in this first layer are integrated into very extensive communication networks by means of the subsequent layers. However, often they were not originally designed for such comprehensive communication relationships. This results in particular challenges with regard to efficient and scalable asset and lifecycle management on the one hand and security-related challenges on the other. The latter are the actual subject of this white paper and will therefore be addressed and described in more detail later.

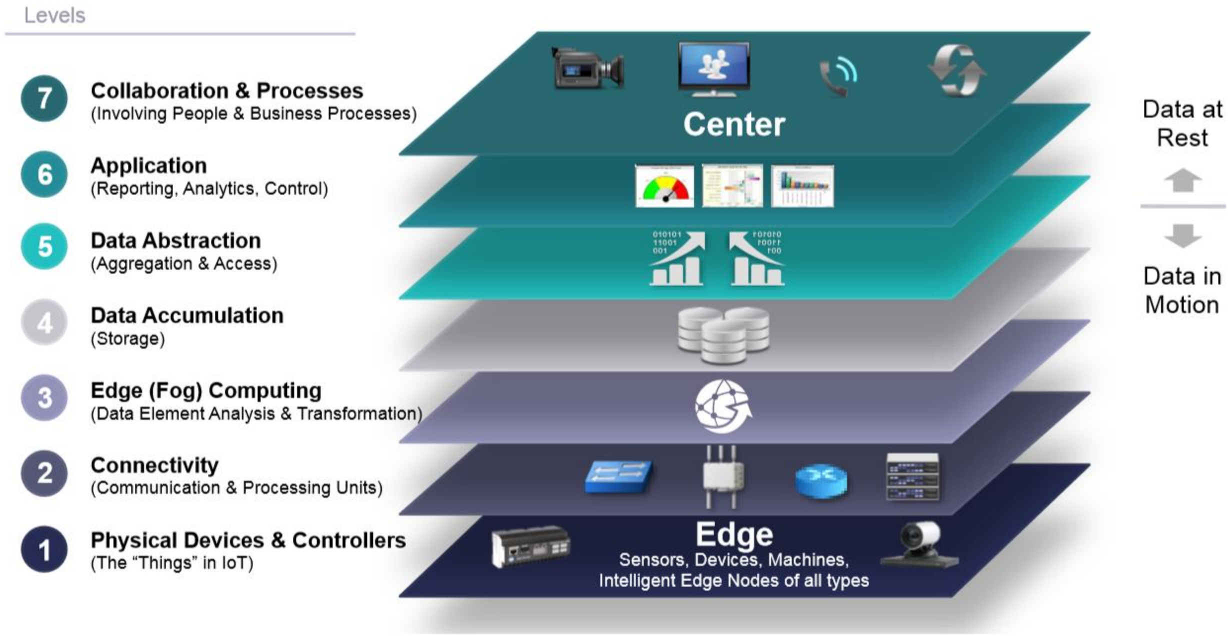
Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge (Fog) Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types
Data at Rest
Data in Motion

Figure 1: IoRT reference model [5]

The **second layer** represents the communication and link layer. It connects the first layer to the network, enables data transport over the network (east-west traffic) and connects the network to the third layer. It is an aspiration of the IoT reference model to leverage existing networks. Since it cannot be assumed that such existing networks use the Internet Protocol (IP), gateways are introduced by means of which the IP capability of the IoT system is established so that all the features of modern IP networks, ranging from routing and switching to network analytics and network security, can be made available to IoT systems.

The **third layer** maps the so-called Edge&Fog computing functionality. This takes account of the endeavor to process data in intelligently designed IoT systems as early as possible or at the point where it makes most sense for technical, business or regulatory reasons - for example, to reduce bandwidth, to meet real-time requirements or to protect intellectual property: either at the edge, i.e., the point at which data is generated, or in the so-called fog area, i.e., the continuum between the edge and the central units such as the data centre or in the cloud. The data processing in the Edge&Fog area includes the following aspects: evaluation of whether data is discarded, persisted in a data historian or forwarded to - possibly different - higher layers, reformatting for consistent further processing in higher layers, possible decoding of encrypted data, possible reduction or combination of data, examination of data packets for security-relevant aspects - keyword: deep packet inspection - and analysis of data, whereby the latter can range from simple threshold value observations to complex analysis with the aid of artificial neural networks - keyword: digital twin. The results of data processing are events or alarms and insights or information. Data processing in the third layer is what is known as in-transit data processing; in contrast to data processing in higher layers, data streams, i.e., data in motion, are examined here.

Not all applications that are to be used for data processing can process data streams, i.e., data in motion, but they require data at rest. This is considered by the fourth layer, the data accumulation layer, by means of which event-based data generation is coupled with query-based data processing. In this way, a bridge between a real-time network and a non-real-time application can be built.

The tasks of this fourth layer are as follows:

- Selection of the persistence type, i.e., non-volatile for long-term storage or in-memory for short-term use.
- Selection of the storage system, i.e. file system, Big Data system or relational database.
- Format conversion, e.g. the conversion of network data packets to entries of relational databases.
- Aggregation, combination and reprocessing of new data with existing data, which can also come from other data sources not necessarily attributable to the IoT system.

One merit of the **fourth** layer is that data may be persisted differently: for example, unstructured raw data streams are stored in Big Data systems - keyword: data-lake - whereas structured data representing events, for example, are stored in so-called data warehouses. There are also other reasons for not storing all data in the same place or in the same system: whether the volume is too large, the data comes from different sources such as an ERP, HRMS or CRM system, or simply because the data is generated at geographically distant locations.

Unifying this heterogeneity of data storage is the task of the **fifth** layer: the so-called data abstraction layer. It enables the development of simple, high-performance applications - hence the scalability of the entire IoT system. The main functions of this abstraction layer are to reconcile different data formats, ensure consistent semantics, ensure the completeness of the data with respect to the higher-level applications, normalize or de-normalize the data and provide it with indexes, protect the data with appropriate authentication and authorization, and make the data accessible using ETL, ELT, or data virtualization.

The **sixth** layer is the application layer, where the dormant data provided by the fifth layer is processed and interpreted - either directly or via integration to an "application abstraction layer", such as an ESB or a message broker. The type of application varies depending on the industry, the business requirements or the nature of the data generating things: Monitoring, control, business intelligence, or analytics systems are typical examples of applications in this layer, although the development and protected, SLA-compliant operation of these applications lie outside the IoT reference model and are addressed by appropriate solutions from the data centre context. In terms of the underlying architecture, a fundamental distinction can be made between monolithic architectures and cloud architectures, the latter involving a certain dynamic in the sense that the functions of the applications are mapped by micro-services which can reside in containers at different times in different locations - e.g., in different public clouds. Appropriate, intelligent control of the data flows can and must already start at the evaluation function of the third layer, Edge&Fog computing.

The **seventh and final layer** of the IoT reference model is the collaboration and process layer. Here, the fundamental aspiration of IoT systems is addressed, that the ultimate goal is to initiate actions that generate a business benefit, address a regulatory requirement, or enhance the security of people and systems, of tangibles and intangibles, or from attacks of any kind. Some actions can be initiated directly by the third- or sixth-layer systems, other actions require integration with higher-level processes or collaboration with humans, whereby the reasons for this can be of different nature: be it because the generated insights are per se intended for further processing in higher-level processes or because they have been generated by artificial neural networks through correlation and therefore, for example, can be used in regulated, audit-enabled processes. In such contexts, they may not be used without the prior assignment of causal relationships by so-called explainers, i.e., human experts who can find precisely these logical relationships based on their expertise. The core function of the seventh layer is thus to enable precisely this collaboration between humans and technical systems as well as the corresponding process integration.

3.2 Special features of the railroad system

The main aspect of this white paper is the topic of IT security and the associated topics of governance, ownership of data, and identity & access management (IAM). The IoT World Forum reference model creates a reference framework that describes seven functional layers, but it does not directly meet the requirements or define them in an architecture. An architecture must be an in-praxi instantiation of the IoT reference model that addresses at least the seven functional layers and that must map data traffic not only logically (from functional layer 1 to functional layer 7) but de facto.

An IoT system in the railroad context - i.e., an Internet of Railway Things (IoRT) - is initially a subset of the Internet of Things for railway-relevant objects. Especially with regard to the critical infrastructure and safety-relevant environments given in the railroad context, the security functions in an architecture as an in-praxi instantiation of an IoRT model deserve special attention. The resulting special features are described in more detail below.

1. Many objects and technologies covered by an IoRT system must have the certification required in the railroad context by the EBA and/or other authorities or be suitable for supporting such railroad processes and certifications.

2. Another distinctive feature - in contrast to other OT environments - is that security concerns do not only refer to the maintenance of operations and the protection of resources and property rights against external influences (e.g. cyber attacks) but also to the prevention of negative effects from the systems on the environment (e.g. the integrity of people). The requirements for functional safety are met by the standards EN 50126 ff., among others according to IEC 61508, IEC 61511 by the introduction of so-called safety integrity levels (SIL). The requirements of cybersecurity are considered, among other things, in accordance with IEC 62443 series or TS 50701 through the introduction of so-called security levels (SL). Depending on the security level, a risk assessment must therefore be different, which means that the design of an IoRT system must also be different: An IoRT system with no or low SIL must be designed disjunctively and separately from other systems with higher SIL and can only be used on the 7th functional level of the IoRT reference model for purely informational purposes. The use of shared infrastructures requires proof of freedom of interference and the appropriate certification. Genuine integration at the 3rd, 4th, 5th, 6th, or 7th functional level, i.e., for example, the creation of a digital twin that can intervene autonomously in rail operations, entails, in case of doubt, the classification of the complete IoRT system in the higher SIL with all the necessary proofs and certification - this will be discussed in more detail in the description of the use cases.

3. A key task of IT/OT security in the rail environment is to protect safety-relevant systems from external influences (e.g., cyber attacks). This can be ensured if security and safety related systems or functions are appropriately separated or encapsulated (e.g., architecturally) and security can be regularly adapted according to the threat situation (systematic application of patches or updates or options for detecting malfunctions or cyber attacks). Security and safety must be separately verifiable and updatable. A standardized security shell is placed around the existing safety world, which can fulfill the requirements mentioned.

Esppecially, the various security measures, which can extend over all seven functional layers, must be specified in an architecture. The absence of a corresponding security functional layer in the reference model provides the opportunity to do this in accordance with regulatory requirements and the relevant company requirements. If possible, modern concepts from the security industry can be taken up in this way - for example, the concept of deperimeterization. This concept assumes that no environment can be completely sealed off - i.e., the identity becomes the perimeter, IAM defines what an identity can do, and analytics - often non-deterministic - such as anomaly detection checks whether these definitions are being adhered to. In organizations with critical infrastructures (CRITIS) in particular, such an approach may not be possible: here, for example, environments with safety-relevant applications must be enclosed in a perimeter and secured by deterministic, auditable measures [6] [7].

The fact that a large number of the devices used are located throughout Germany without physical access protection makes it more difficult to meet the requirements listed here or to deal with the special features. Furthermore, the devices are used both in vehicles and on the infrastructure. Particularly in the area of vehicles, there are more than 400 railway undertakings (RUs), and with transit traffic, more than 1000 RUs. It must be possible to exchange information with them to leverage the benefits. At the same time, this makes it more difficult to meet the requirements.

3.3 Threat scenarios

A comprehensive threat analysis for the overall system must be done independently and requires consideration of the overall system.

However, particularly relevant threats can be identified for IoRT devices, which, if exploited by an attacker, become a threat and, with an opportunity, a risk. The top ten threats for Industrial Control System Security (ICS) from the BSI [8] are described below; the attacker types are not explained in detail, but the possible risks are described in the following chapters as examples.

1. infiltration of malware via removable media and external hardware
2. infection with malware via the Internet and intranet
3. human error and sabotage
4. compromise of extranet and cloud components
5. social engineering and phishing
6. (D)DoS attacks
7. control components connected to the Internet
8. intrusion via remote accesses
9. technical malfunction and force majeure
10. compromising of smartphones in the production environment

4 Applications of standard IoT in the railway context

4.1 Introduction

There are a variety of potential application areas for IoT in the railroad context. In many cases, these follow the standard requirements of Industrial IoT (IIoT) and can therefore also be handled with the same solution approaches from an IT security perspective. For a more in-depth look, three examples are shown below (Figure 2).

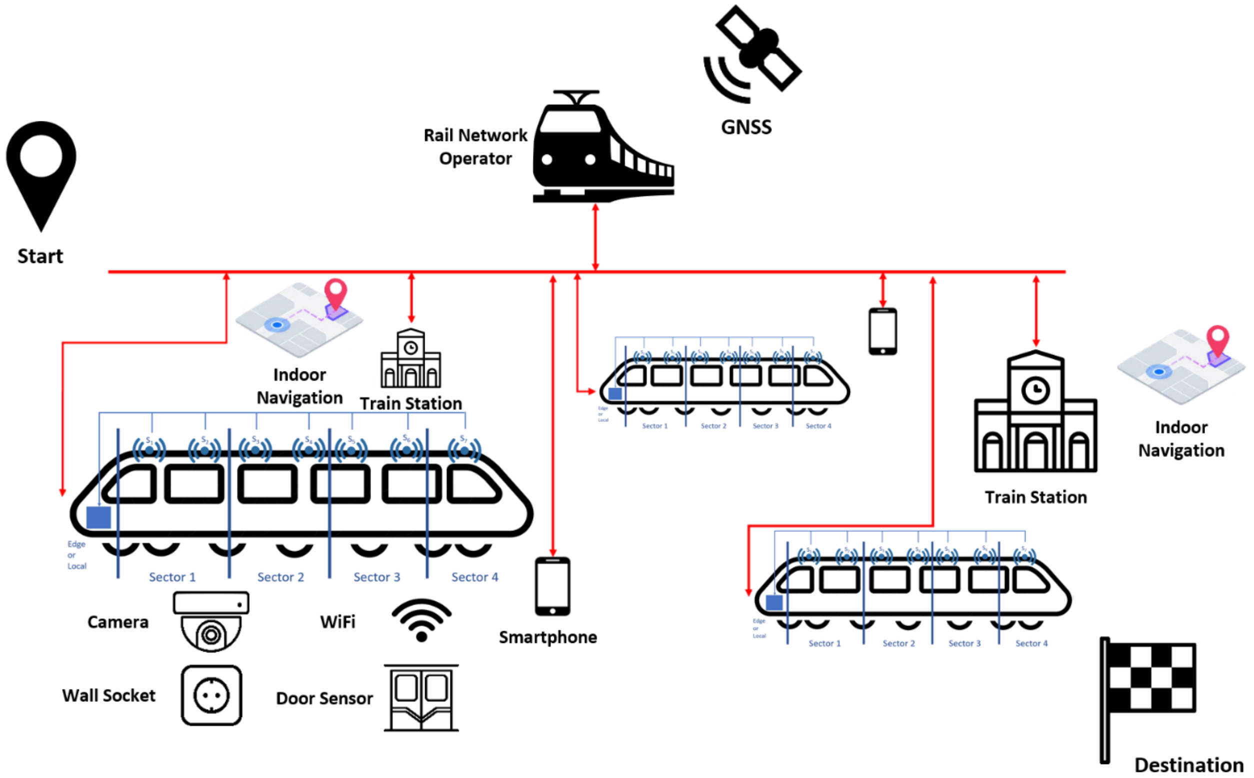

Figure 2: Overview of the standard IoT components used in the railroad context

4.1.1 Use case 1: Optimization of passenger distribution

Rail passengers are often not equally distributed along the train, but form crowded areas. This is due, to the location of station entrances and exits and, in some cases, to additionally attached coaches. This causes delays in boarding and disembarking, especially at peak times, which could be prevented if passenger distribution were improved. The networking of sensors within the train allows live analysis of passenger distribution and its optimization. For this purpose, each train is divided into sectors delimited by camera systems or light barriers. Each sector independently determines the passenger volume via sensors and reports this to a central control unit. The latter is installed in the train or represents the edge computing unit. The sector size and its spatial distribution determine the ideal passenger load factor a priori. The central control unit optimizes sector utilization live and directs passenger flows to underutilized sectors through the screens located on the train or displays mounted on the platforms. This enables the best possible positioning of passengers at the edge of the platform at an early stage, reducing boarding and alighting times. As an alternative to the above-mentioned data sources, it is conceivable to evaluate the station's own Wi-Fi or the usage of wall sockets to estimate the distribution of passengers. The decisive disadvantage here is the lack of reliability, since not every passenger uses the Wi-Fi or is connected to a power outlet. Consequently, passenger distribution estimates derived from this cannot be prioritized.

IT security aspects:

- Cameras: privacy, personal data (confidentiality), attachment of an image / own video image from a similar perspective.
- Evaluation system/classifier: deception of facial, body recognition, injection of a manipulated video stream

- Wi-Fi: MAC address, fingerprint, manipulation: all connect to the strongest signal (man-in-the-middle)
- Light barrier: protection against manipulation/misuse (interruption of the barrier by passengers, although no person has entered, to “reserve” more space)

4.1.2 Use case 2: Violence prevention through automated camera analysis

Movement patterns and facial features allow conclusions about a person's emotional and mental state. Vandalism generates high annual costs. Passenger safety is closely linked to the willingness to use railway operator’s travel services, which is why security services have been intended to guarantee a minimum level of security. The problem here is the localization of dangerous situations within the train. Security personnel are usually located at the end of the train or walk around the train on patrols. The networking of camera sensors allows early detection of scuffles or harassment by evaluating gestures and movement profiles. For this purpose, the data is processed on the train or "on-the-edge" with the help of artificial intelligence and then sent to the operator’s backend. This informs the security service within the train immediately or also at stations about dangerous situations.
IT security aspects:

- Cameras: data protection (privacy), personal data (confidentiality), attachment of an image/own video image from a similar perspective.
- Evaluation system/classifier: deception of face, body recognition, feeding of a manipulated video stream, architecture: centralized/decentralized (14*10 cameras), adaptive evaluation rate (trend development: evaluation with higher frame rate if a trend emerges)
- Connection between cameras and evaluation system: access to, manipulation of the video stream.

4.1.3 Use case 3: Optimization of the travel experience by creating a travel profile

The travel experience can be enhanced by using a smartphone app that accompanies the user from their starting point to their destination, suggesting walking routes and the use of all available modes of transportation.
In doing so, the user is provided with individual real-time-based recommendations for the itinerary, trip planning, and wayfinding dependent on the immediate environment (for example, through arrows in an augmented reality display on the smartphone). These recommendations are based on

- The current traffic situation (delays, cancellations, capacity utilization),
- the user's previous personalized travel behavior
- as well as fine-granular indoor and outdoor navigation.

In addition, the user also receives information on which public transport stop to get off at. Another advantage for the user results from the arrival time estimation and the route description for different alternative travel routes and means of transportation during the trip. Thus, a user who is already on the train can check whether, for example, the route

- platform -> exit station -> public transport -> exit/stop -> walk -> hotel or the route
- platform -> exit station -> cab stand -> hotel

is better. This can be used to optimize fares and weigh up travel duration and fare, as well as other criteria such as taking along a bicycle, bulky items of luggage, disabled access, etc.

The app provider/travel service provider can use travel profiles to make statements for fine-grained demand planning regarding vehicles, their capacity, the number of trains, the expansion of new routes, and even the size of stations and measures for persons with limited mobility.
In this context, the current and forecast utilization of the infrastructure (platforms, trains, buses, streetcars) can be determined in high temporal resolution with the aid of image analysis from cameras installed on the trains, on the platforms and in the station. This information can be used to plan construction sites

and reconstruction work at stations. It can also be used to direct passenger flows to alternative routes, such as via another building level, in the event of short-term disruptions, such as the failure of an escalator. Finally, the profiles can be used to optimize fares accordingly.

IT security aspects:

- Profile information: App, personal data (confidentiality), movement data.
- Smartphone: manipulation of sensor data, identity theft
- Manipulation: falsification, withholding of occupancy data by transportation companies to acquire more customers
- Cameras: privacy, personal data (confidentiality),
- Evaluation system/classifier: deceiving face, body recognition, feeding a manipulated video stream

4.2 Solution

The presented use cases impose requirements on different areas of IT security, such as data privacy and data integrity. Privacy is important as soon as camera-based intelligent systems, as described in the second use case, are deployed or personal data, such as motion profiles, as described in the third use case, are stored.

However, these outlined use cases show that they have hardly any special requirements from an IT security perspective, despite their clear connection to rail operations. Use cases that require special measures because they are related to rail operations are analysed in the next section. Nevertheless, the conventional security measures that are common in the "convetional" IoT must also be applied in these use cases. These include encryption and authentication of any network communication, whether between the cloud server and the customer's smartphone, or between sensors (e.g., cameras) and evaluation units, as in passenger distribution or the violence prevention example. Changes to the configuration data of the system and all its components must be authorized to prevent manipulation by third parties. Measures such as passwords or even two-factor authentication serve this purpose, as does the physical blocking of interfaces such as USB ports.

Furthermore, it is important to check the IoRT devices for malware in order to be able to detect and eliminate it in time, as the infiltration of malware is currently one of the most common threats to digital systems. It must be possible to eliminate discovered vulnerabilities remotely by applying patches/updates. Manual procedures, which are still common in some cases for larger technical systems, can no longer be a solution given the volume of IoT elements. These updates are not only necessary to protect the IoT devices themselves, but also to prevent abuse for bot networks for DDoS attacks.

One special feature we would like to highlight with the use cases is the secure processing of personal data, for which the requirements of the EU General Data Protection Regulation (EU GDPR) must be complied with in a mandatory manner and the implementation must be demonstrated. This includes measures such as description of the purpose limitation of the processing, data economy, appropriate deletion periods and the implementation of "appropriate technical and organizational measures". Technical measures are all attempts at protection that can be implemented physically in the broadest sense or that are implemented in software and hardware, while organizational measures are those attempts at protection that are implemented by means of instructions for action, procedures and approaches. These can include, for example, the physical deletion of data, cryptographic encryption or internal IT and data protection regulations.

To put the threats into context on the described use cases and show their relevance, we used the top 10 ICS threats and countermeasures published by the BSI. In Table 1 below, we assign which threats apply to which use cases currently - as of 2020. The BSI document also describes countermeasures that can be implemented for our use cases to counter the threats.

		Passenger distribution	Violence prevention	Travel profile
1	Infiltration of malware via removable media and external hardware.	yes	yes	yes
2	Infection with malware via Internet and intranet	yes	yes	yes
3	Human error and sabotage	yes	yes	yes
4	Compromise of extranet and cloud components	yes	yes	yes
5	Social engineering and phishing	(no)	(no)	yes
6	(D)DoS attacks	yes	yes	yes
7	Control components connected to the Internet	no	no	yes
8	Intrusion via remote access	yes	yes	yes
9	Technical malfunction and force majeure	(yes)	(yes)	(yes)
10	Compromise of smartphones in the production environment	no	no	yes

Table 1: Relevance of ICS threats by BSI per use case.

To determine the extent to which a threat applies to the use case, we use the following, generic, definitions for the services provided in the described use case:

- Passenger distribution: the occupancy of the train is correctly displayed on the platform.
- Violence prevention: A dangerous situation on the train between passengers is correctly detected.
- Travel profile: recommendations for walking routes and means of transport are correctly suggested.

In the following, the threats from the top ten list [8] are specified for the use cases described above.

1. *Infiltration of malware via removable media and external hardware*: Especially for the devices that process the sensor data to produce a result, malware can be infiltrated through connected removable media. In the case of passenger distribution and violence prevention, it can be assumed that such an evaluation unit is installed on the train and can be influenced by malware. In the case of the travel profile, the operator can hardly influence possible malware on the user's terminal device (smartphone). However, the collection and evaluation of the raw data to generate the recommendations are within its sphere of influence. The devices used for this purpose are also exposed to the threat of malware.
2. *Infection with malware via the Internet and intranet*: in order to provide the service in the passenger distribution and violence prevention use case, it is not absolutely necessary for the system to be connected to the Internet, but it is definitely necessary to have some form of network in order to communicate the load to the next station or to report detected dangerous situations to the security service. Malware can spread via this network (intranet). For the travel profile case, the Internet is naturally required to reach the end user, so the threat of malware also applies from the Internet.
3. *Human error and sabotage*: human error and sabotage can rarely be ruled out. A passenger could try to fool the door sensors to falsely provoke a higher occupancy. As a result, at the next station, the occupancy is not correctly displayed, and passengers may not distribute themselves optimally across the platform. Terminal devices are subject to sabotage on various levels. Cameras, for example, can be destroyed or sprayed with paint to prevent recording. In addition, the evaluation can be deliberately deceived, e.g., by artificially increasing the utilization level of the attackers' travel profile by using a large number of smartphones in order to provoke other, poorer recommendations.

4. *Compromising extranet and cloud components*: All the use cases described involve cloud components that evaluate and process data in the background. Therefore, this threat applies to all use cases.
5. *Social engineering and phishing*: Social engineering and phishing are multi-layered threats. For both passenger distribution and violence prevention, it can be argued that access data cannot be spied out because there are no user accounts or workstations with, for example, e-mail access. On the other hand, social engineering or phishing attacks on maintenance staff dealing with the devices are conceivable, which are influenced to reveal maintenance access or to change configurations in the attacker's sense. Travel profiling and resulting recommendations require a user account whose credentials can be spied on through phishing emails. In addition, the back-end system may be a lucrative target for attackers who perform social engineering or phishing to manipulate the system. Appropriate protection through staff training and notices to customers, organizational measures and a reporting system is required here.
6. *(D)DoS attacks*: In all presented use cases, DoS attacks can be carried out by interrupting the wireless communication between train and trackside or with the end customer by jamming. Such jamming attacks can hardly be prevented, instead the operator is forced to find the jammer to remove the interference. DoS attacks on the devices themselves are already hampered in the case of passenger distribution and violence prevention due to limited accessibility (no Internet). General measures against DoS attacks include redundant design of devices and connections and/or appropriate over-specification of resources.
7. *Control components connected to the Internet*: The threat from Internet-connected control components can be easily eliminated for passenger distribution and violence prevention use cases by not connecting the components to the Internet since it is not required. Due to the large spread and networking in the travel profile use case, it will not be possible to avoid components being accessible via the Internet here. These should be secured accordingly by access protection and continuous mitigation of security vulnerabilities.
8. *Intrusion via remote access*: nowadays, cameras, sensors, end devices and devices at all levels of the Internet of Things have remote maintenance access, which - if not correctly protected - can become a gateway for attackers. Therefore, all used remote maintenance access should be protected with effective authentication and authorization, and unused remote maintenance access should be deactivated.
9. *Technical failure and force majeure*: Technical failure and force majeure cannot be ruled out, of course, but they apply to a large number of systems and are not part of the consideration in this white paper, which is intended to deal with IT security attacks.
10. *Compromise of smartphones in the production environment*: we assume that the threat from smartphones in the production environment can be ruled out in the case of passenger distribution, since no smartphones are involved in any part of the service. However, in the case of violence prevention (alerting security personnel) and travel profile (recommendation to the customer), smartphones are present in the scenarios. In the case of security personnel, these are devices owned by the operator, so there is extensive leverage here to address malware and compromise. In the case of the end customer, however, these options are not available, so that the sphere of influence is limited at most to the application installed by the user.

5 IoRT applications with special requirements

5.1 Introduction

Digitalisation of the railroad infrastructure and networking of the command and control systems are the basic requirements for the use of IoT in railroad operations, in short: IoRT. The introduction of this new technology builds upon so-called digital interlocking (DSTW) and the NeuPro architecture.
In the following, example applications considering the specifics of such IoRT systems are described including related benefits and challenges. One possible solution, especially in combination with or in the immediate vicinity of safety-critical systems, is the separation approach. This is explained in more detail at the end of this chapter. Explanations of the systems dependencies, possible separation strategies and technological approaches to this have already been developed and published in earlier documents [9] [10].

5.2 Future interlocking technology and NeuPro architecture

The NeuPro architecture [11] defines a digital interlocking system (DSTW) and enables the control commands to be transmitted to the field elements such as points and signals by means of information technology (IT), e.g., via an IP network and standardized interfaces.
Figure 3 roughly depicts this architecture for the DSTW.

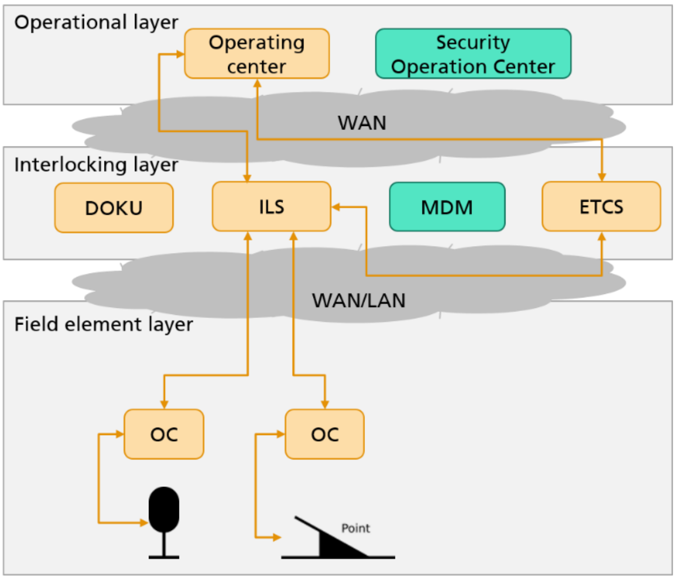

Figure 3: NeuPro/DSTW Architecture (based on [11])

The architecture consists of the safety components (in orange), which are responsible for safe railroad operation, and the security components (in green), which implement additional functions to protect the railroad infrastructure from cyber attacks. The components are divided into three levels - operational, interlocking, and field element.
- At the operational level, there is the command and control centre (CCC) and the security operations centre (SOC). The operations control centre is responsible for steering and controlling rail operations. Among other things, the execution of train movements is controlled here. The SOC is responsible for processing infrastructure messages and detecting security-related events.
- The most important safety systems, such as the DSTW (cf. ILS), Maintenance and Data Management System (MDM), and DOKU, are located at the interlocking level. The DSTW checks the routes from the operations centre, determines required technical dependencies and “sets” the routes by sending commands to appropriate field elements (start and end signals). In addition, the DSTW processes the messages from field elements and, in the event of an error, e.g., technical faults, it switches to the safe state (fail-safe). In this case, the route is blocked until the signal dependency can be restored. The MDM system is responsible for providing the update files (e.g., new configurations) for the field elements. In addition,

the MDM forwards the security-related messages to the SOC. The DOKU system is a kind of historical database that logs all safety-relevant events. These logs are used in the analysis of safety incidents. The interface to the European Train Control System (ETCS) allows the necessary operational information to be exchanged between the vehicle and the infrastructure.
- The field element level includes the object controllers (OC), which control elements of the trackside equipment such as switches/points, signals, or level crossings. An OC is usually connected to a single element using analog signals and converts the digital commands from the DSTW to safeguard the routes as well as the analog feedback signal from the element to the DSTW, accordingly. As a rule, the OC has no "intelligence" of its own.
All components in the DSTW system are interconnected up to the OC via the railroad WAN, i.e., Ethernet- and IP-based transport network (LAN or WAN). In this context, the communication for railroad operations can be performed using the RaSTA [12] protocol to ensure reliable delivery of messages and the necessary resilience.

5.3 Selected use cases

In the following, two use cases from the area of control and safety technology are described and the relevant aspects of IT security are analysed.

5.3.1 Use case 1: IoRT for condition-based and predictive maintenance

Condition-based maintenance (CbM) and prediction-based (or predictive) maintenance (PbM) is an on-demand or condition-based maintenance process based on the evaluation of data regarding the actual condition of railroad systems and equipment.
In CbM, various operationally relevant parameters are automatically recorded by sensors. In PbM, which is a further development of CbM, the available data is evaluated with the aid of special models and algorithms in order to make the most accurate prediction for the time of the next required maintenance for the component. Data-based maintenance approaches can be used to achieve various goals, such as increasing the efficiency of the process thanks to advance planning, saving costs, increasing the safety of operations and reducing downtime [13]. In this white paper, the focus is particularly on minimizing unplanned disruptions.
Predictive maintenance includes the following steps:

- the monitoring of system health and the environment using sensors,
- the collection, processing and transmission of data,
- the storage and analysis of the collected data,
- the prediction of specific events (such as failure or malfunction).

Despite the use of IoRT, maintenance activities as well as servicing can never be completely eliminated, as they are subject to normative and regulatory requirements. Thus, IoRT is a supporting measure for railroad operators, which can help extend the pre-defined maintenance periods, minimize the probability of failures and increase the availability. IoRT offers the greatest technical added value in the area of inspection, because with the help of sensors and CbM, the actual condition can be automatically controlled, checked and documented without a manual on-site inspection. IoRT delivers the greatest operational added value in the area of PbM, with which the maintenance of facilities and trains can be optimized so that it is carried out at the most favorable time. In this way, necessary material and personnel are available on time and there are no unplanned effects on regular operations.

5.3.1.1 System architecture for IoRT-based maintenance

A possible architecture of the predictive maintenance service is shown in blue in Fig. 4. The IoRT sensors used by the service are shown in a separate sensor layer in yellow.

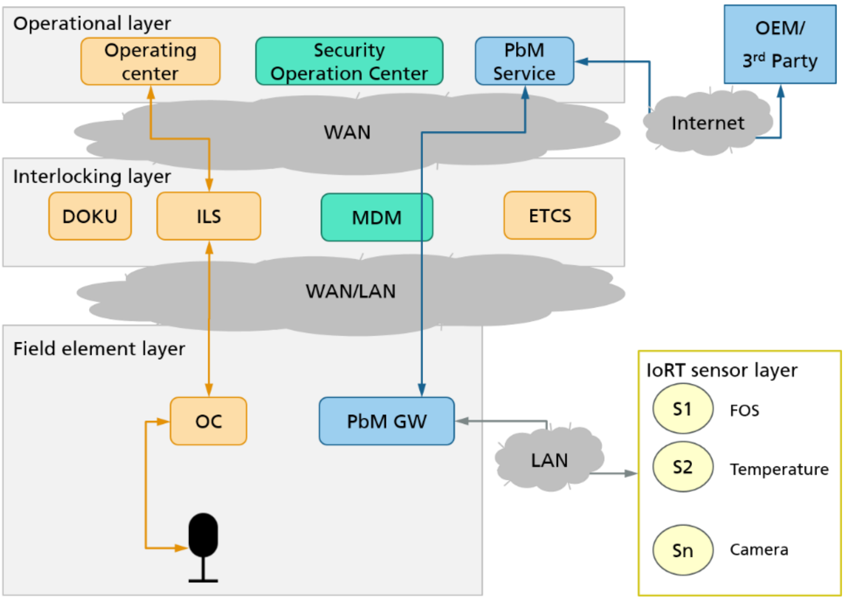

Figure 4: IoRT-based maintenance services

Here, the IoRT sensors are used to monitor the actual state of command and control systems and their environment. Depending on what physical values (e.g., temperature or humidity) or information are needed to calculate predictions for a particular component, various commercially available sensor types can be used. For example, fiber optic sensors (FOS) installed along the railroad track allow monitoring the operational status of tracks and can serve as IoRT sensors at the same time.

The PbM application on a dedicated Io(R)T Gateway (GW) (cf. Fig. 4) acquires the data from the connected IoRT sensors, converting the analog signals into digital ones if necessary. The PbM application can additionally process the sensor data like FOS data locally, e.g., by forming a dataset with a time stamp or also with additional information like temperature or camera image. In order to be able to use the condition information available for predictive maintenance, the PbM application forwards the acquired data and prepared datasets to the PbM service in the operations centre. The PbM application can also be actively queried by the corresponding service in the operations centre if required. PbM-relevant communication with the PbM service within the operating organization of the infrastructure's manager takes place via a protected railroad WAN (IP network). The operations centre collects and stores the information on the current state of the assets to enable prediction of failures and malfunctions and reporting, as well as to provide prompt information exchange between operational processes.

The PbM service can also correlate the received sensor data with other information, such as the safety state of the field element or the safety application (object controller), as well as the security alerts from the SIEM (Security Information and Event Management) system to enable a comprehensive assessment of the tracks condition and to reduce the probability of false predictions.

The PbM service can also provide access to raw sensor data from the PbM application or pre-processed assessment reports to authorized external stakeholders, such as equipment manufacturers (see OEM in Figure 4). This functionality can implement data filters to enforce access permissions (data governance) and preferences when forwarding information, thus, also enabling compliance to the requirements of the GDPR. This is particularly important for the exchange of information with entities external to the railroad operator and is mandatory by law.

The PbM service provides an Internet interface for communication with external players located outside the railroad WAN.

5.3.1.2 IT Security Aspects

i. Threat analysis based on BSI ICS Top 10.

The list of top 10 threats [8] can be mapped to the IoRT based PbM services/systems use case as follows.

1. *Infiltration of malware via removable media and external hardware*: the use of removable media can be prohibited without loss of functionality in the proposed PbM system and the corresponding interfaces can be disabled. In this context, data exchange and updates should be performed securely via an appropriately protected WAN. In contrast, IoRT sensors and even the PbM gateway in the track area can be replaced by infected or compromised components by the local attacker. Such compromised components can, among other things, provide false data regarding the condition of the equipment.
2. *Infection with malware via Internet and Intranet*: As a highly networked system, PbM can be infected by malware. Non-targeted malware (e.g., worms or Bitcoin miners) can impair PbM functionality by limiting system processing power or rendering necessary data unusable or deleting it. In the worst case, the PbM service is no longer accessible. Particularly dangerous is targeted malware that is delivered, for example, as part of the manipulated update, and either enables unauthorized access to systems and data, or feeds them with incorrect information (e.g., input data, procedures, or models), or manipulates these systems and data in such a way that the predictions are falsified without these manipulations being noticed.
3. *Human error and sabotage*: the PbM system can be compromised by misconfiguration and misoperation of the components or networks that enable communication between different levels of the system. For example, IoRT sensors can be disabled or replaced, the configuration of the PbM application can be changed to prevent certain data from being queried or forwarded, or this data can be incorrectly timestamped so that it appears irrelevant for the performed malicious action. This also applies to the PbM service. By sabotaging the Internet interface, the restriction set up with the help of data filter rules can be lifted, so that complete data records relating to the facility's state can be disclosed in an uncontrolled manner.
4. *Compromise of extranet and cloud components*: The architecture for the PbM service does not include any decisions about the concrete realization of this service. The only external interface is the interface to the external actors that can send requests to the PbM service in the operations centre via the Internet. These requests can be manipulated or deleted by an attacker, which will have a negative impact on service quality for the external parties.
5. *Social engineering and phishing*: This threat can lead to disclosure of access credentials or other IT security-related information in the PbM system. In addition, the attacker can even gain unauthorized access to the PbM service in the operations centre using methods of social engineering and phishing.
6. *(D)DoS attacks*: The correct operation of the PbM service in the operations centre depends on the data that the service receives over WAN from the IoRT sensors at the field element level. (D)DoS attacks on network connectivity can hinder the service from collecting up-to-date information about the state of the assets. The delay and possible loss of this data due to the overfilled distributed storage may also have negative consequences for the prediction algorithms and forecast calculation. The PbM gateway hosting the respective application, as well as the PbM service (e.g., database and server), can also be disrupted or crashed by certain messages.
7. *Control components connected to the Internet*: The PbM system does not allow direct connection of control and command components to the Internet.
8. *Intrusion via remote access*: As the PbM system relies on the WAN for communication, attackers may be able to gain access to this system via remote maintenance access.

9. *Technical malfunctions and force majeure*: failure or incorrect function of the PbM service due to defective hardware or software components cannot be ruled out. This applies in particular to components in the track area exposed to challenging environmental conditions.
10. *Compromise of smartphones in the production environment*: the primary objective of the PbM system is the collection and processing of information, not the control of equipment with or without remote maintenance access. Therefore, this threat is only relevant if the smartphones are used as sensors, which is unlikely due to the related high cost.

ii. Risks

In order to meet its objectives and achieve improvement over the state of the art, the IoRT-based PbM system must provide reliable information that corresponds to the state of the observed command and control system.

If the PbM generates incorrect failure prediction, it may lead to the increase of maintenance costs due to additional unnecessary inspections, facility shutdowns, or investments (e.g., in renewal or repair instead of maintenance). If, to assess the operational status of the affected system, railroad operations have to be restricted or suspended in an unplanned manner, this will have a negative impact on punctuality and allocation of the necessary resources.

The financial impact of such a situation can be estimated high. The likelihood, without protection, is "very likely". In addition, the reputational damage is likely in case of the disclosure of such events to the public. The effects of such damage are long-term and can only be estimated with difficulty.

The above situations can occur if a system is incorrectly classified in the prediction as a "system requiring maintenance" or "system with limited operational capacity". The opposite case is also possible: the system on the verge of failure may be incorrectly assessed as healthy. This poses a risk to safe rail operations, in addition to the financial damage. The potential damage to the operator in this case depends on whether the periodic manual inspections are performed by well trained personnel as well as the standard maintenance procedures prescribed by state authorities continue or whether they have been discarded for cost reasons and due to the high confidence in the PbM system. The problems missed by the PbM system may still be detected and corrected in time during a scheduled manual inspection, while the legal requirements are also met in the process. Should "double" inspections be dropped, such classification errors of the PbM may not only have legal consequences, but in the worst case may also result in an accident and even impairment of personal integrity.

In this respect, these risks clearly have an impact on both the company's resources and its operational safety. Thus, only sufficient consideration and evaluation of the risks and taking adequate protective measures can allow the use of IoRT to serve improvement or optimization.

iii. Assets and protection goals

As the discussion above shows, the IoRT sensor data, the datasets compiled by PbM application, and the PbM service predictions based on them play a critical role in safe rail operations and must be protected accordingly. The authenticity and integrity of the data are particularly important, e.g., that they have been verifiably generated in the IoRT system and have not been modified in an unauthorized manner. For example, if an attacker manipulates or falsifies the sensors monitoring the condition of the tracks or the measurements themselves, it could result in the PbM service generating incorrect failure predictions and inappropriate responses. In addition, software and hardware configurations such as prediction methods and models, filtering rules, and access permissions, as well as the software and hardware itself that enable the functions of collection, processing, storage, and transmission of PbM data, are worth protecting.

Availability of information is necessary to ensure quality of service. Missing data can lead to classification errors and may be interpreted as a railroad system’s failure. This can be abused by an attacker to trigger expensive countermeasures and in this way harm the operator.

Since sensor data does not contain personal information or trade secrets, they are usually not considered confidential. Therefore, confidentiality is usually not prioritized as a protection goal. However, these data allow a third party to draw conclusions regarding the condition of the railroad assets, especially if additional background information such as track plans or specifications for the field elements or facilities are available. For this reason, the infrastructure manager should consider protecting the PbM relevant data from unauthorized access and disclosure.

The architecture of the PbM service in Figure 4 provides many entry points for the potential attacker. Attacks are possible at the sensors and the PbM application, at the IoRT gateway in the track area, the PbM service in the control centre, and at the communication links between the systems. Assuming that communication between the PbM application in the track area and the PbM service in the operations centre takes place over a WAN cleared for safety-critical data transmission, it can be assumed that this communication is appropriately secure. Furthermore, it is assumed that the transmission components, other than the IoRT devices themselves, have adequate physical access protection, e.g., through access control systems or appropriate detectors that can be correlated with scheduled work on the devices. This would allow local attacks and manipulations to be detected in time or effectively prevented.

5.3.2 Use case 2: Local situational awareness (SE)

The local situational awareness (SE) service enables the detection of threats and their evolution over time based on information from the nearest environment and on-site decision-making about local rail operations using this knowledge. IoRT sensors provide in this case a source of this information. Such SE service represents a safety-critical extension of today's DSTW functions.

Currently, once the track has been locked, the interlocking can only process the fault signals from OCs and block the particular section of track. There is no way to automatically detect and respond to the local disturbances such as foreign objects in the track area or on the track. Now, it can be assumed that the IoRT sensors are installed along the track and connected to a nearest IoRT gateway depending on their range. When the sensors or the corresponding SE application on the gateway detect (by correlating data from multiple sources) an obstacle on the tracks, the operations centre can be informed to initiate an emergency stop order or close the corresponding track before a train enters the section. The centre can provide this information to the driver using an ETCS L2 interface or shorten the Movement Authority (MA) so that the train can be stopped in time before the hazard point.

Accordingly, IoRT sensors can help gather real-time information about the situation on the track, identify potentially dangerous situations, and initiate the necessary actions based on this information. This would allow rail operators to remedy disruptions efficiently and to avoid potential hazardous situations as well as to further advance the automation of rail operations. For example, FOS sensors can detect dangerous objects (tree, herd of sheep, person, etc.) in the track area in addition to monitoring the track’s condition. Possibly, other Io(R)T sensors, such as an IP camera, can be used in conjunction with FOS to improve detection results.

5.3.2.1 System architecture for IoRT based situation detection.

The components and communication links that make up the IoRT-based SE service are shown in red in Figure 5.

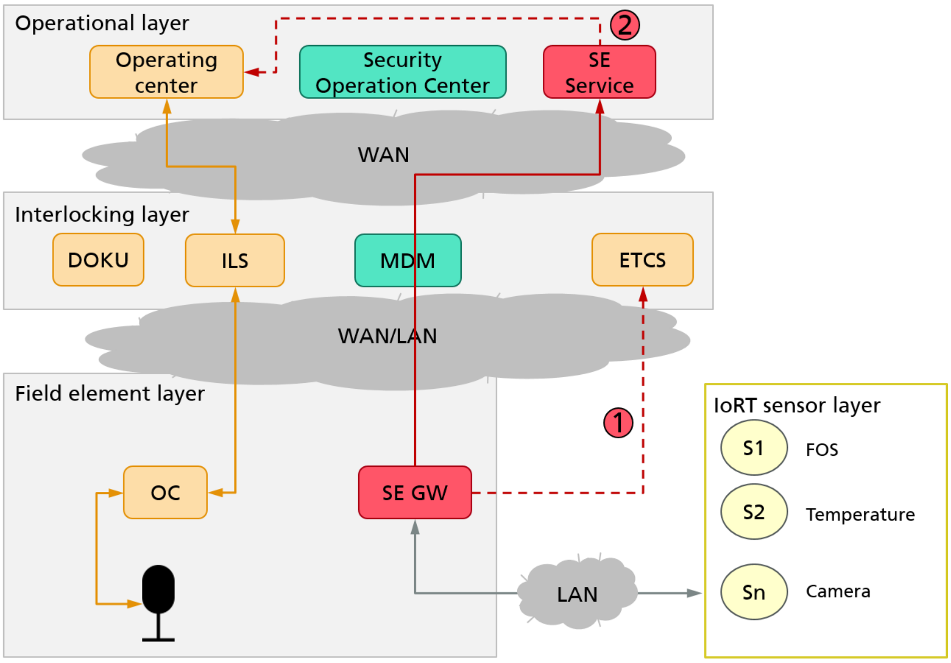

Figure 5: IoRT based service for situation detection in the track area

The SE application on a dedicated IoRT gateway (in Figure: SE GW) collects data from the sensors in its network; in the case of analog sensors, the signals are converted to digital. The SE application processes and analyses the sensor data locally to detect safety-relevant events on the track in real time. Since the gateway's computing power is limited, the decision-making process can also be supported by an SE service in the operating centre. The SE service also collects information from multiple track sections and analyses it to identify threat evolution patterns and predict hazards. The service also provides the corresponding alerts for the integrated operator workstation in the centre.

If such a safety-relevant event is detected, the SE application can react autonomously. The aim is to prevent trains from entering the potentially hazardous track section. Since the SE application does not know the positions of the trains, the following steps must be performed to ensure the operationally safe state (fail-safe):

① The SE application sends a notification to the RBC, which can reach the on-board unit or the driver and request the train to stop in time.

② The SE application sends information to the "Operation Centre", for example the operations centre or the TMS (Traffic Management System), to inform either the affected driver and/or other drivers depending on the current situation and, if possible, to specify a different route.

The corresponding information flows are marked by red arrows in Figure 5 and numbered accordingly.

To avoid interference with safety-critical functions, the SE application can alternatively send an alarm to MDM or SOC, which in turn can inform the operations centre about the detected problem in the usual way.

Communication between the SE application at the field element level and the SE service at the operations centre takes place over the infrastructure operator's WAN.

5.3.2.2 IT security aspects

i. Threat analysis based on BSI Top 10

In the following, the threats from the top ten list [8] are mapped to the IoRT based SE service/system use case. Many findings here are similar to the previous command and control use case. The main difference between the use cases is that the real-time information from the SE application has higher operational relevance as it is immediately relevant. Therefore, the threats that affect the real-time transmission of this information are also of higher relevance.

1. *Infiltration of malware via removable media and external hardware*: as already explained for the PbM service, the IoRT sensors and the gateway in the track area are exposed to a particular risk. Removable data carriers are not needed for the SE functionality and must not be used.
2. *Infection with malware via the Internet and intranet*: as in the case of PbM, the SE service uses communication networks and is vulnerable to such attacks. A prompt reaction to the current events plays a more important role in the SE service than in predictions, which is why the malware that affects the reaction time is also more dangerous. In the SE case, the decision-making involves multiple distributed information sources and is less vulnerable to infection or manipulation of individual components.
3. *Human error and sabotage*: the findings for the PbM system also apply to the SE service. The exception is the Internet interface to the outside world, which is not present in this case. The SE service provides a strong incentive for malicious actions because, if successful, they allow the attacker to disrupt or stop rail traffic in a given area. This highly visible effect would be reported in the press and is especially attractive to script kiddies motivated by fame or disgruntled employees.
4. *Compromising extranet and cloud components*: A connection to the cloud is not defined for the SE service. Although some rail operators want to outsource their safety-critical applications to the cloud, these are then on-premises systems. Thus, these as well as the SE components in the field element layer do not have access to other networks except the rail operator’s WAN and therefore cannot be directly connected to a public cloud.
5. *Social engineering and phishing*: the findings from the PbM use case also apply to the SE service.
6. *(D)DoS attacks*: Since the SE application can in many cases process the sensor data locally, lack of communication with the operations centre can only delay the response. In this case, the SE application can use the interface to the RBC of the ETCS to inform about the potential danger for rail operation. Since the SE service collects data from multiple distributed sources, a temporary breakdown of one SE gateway can be managed. Like PbM, the gateways hosting the SE application as well as the SE service can be disrupted or crashed by certain messages.
7. *Control components connected to the Internet*: The SE system does not allow direct connections of control and command components to the Internet.
8. *Intrusion via remote access*: the findings from the PbM use case also apply to the SE service.
9. *Technical malfunctions and force majeure*: The findings from the PbM use case also apply to the SE service. Since the components in the field are especially vulnerable due to changing environmental conditions and lack of control by personnel, and since these very components are responsible for local decision-making, additional safeguards should be implemented to prevent false positives due to defective components.
10. *Compromise of smartphones in the production environment*: this threat is relevant if persons in the tracks area would be detected based on their usage of smartphones. In this case, the attacker can use tailored smartphones to fake certain situations. However, the scenario is not realistic.

ii. Risks

Similar to the previous use case, the reliability of information plays a very important role for the SE service. Manipulation of IoRT sensors or the transmitted data by an active attacker can lead to two undesirable outcomes. The SE application may fail to detect an obstacle (in time) and positively influence the traffic (false negative). In this case, the standard safety measures currently in place are available, but may not be sufficient to prevent an incident. Depending on the severity of the incident, this could have catastrophic consequences for the rail operator.

In an alternative case, the attacker may trick the SE application into detecting an obstacle where there is no obstacle at all (false positive), or misjudge it, causing a critical response to a dangerous situation (false negative). On the one hand, this reduces confidence in the system and on the other has negative consequences for the operator. In particular, delays are to be expected due to the unplanned and unnecessary impairment of traffic and the securing of alternative routes. If the attacker succeeds in manipulating several SE applications at the same time, it may also lead to regional or large-scale disruptions of operations. This in turn would be associated with high financial damage and loss of reputation. Additional investment in this SE service is also likely to be detrimental if it fails to gain acceptance due to high error rates.

iii. Assets and protection goals

Accordingly, in this use case, the IoRT sensor data, the datasets compiled by SE application, and the assessments based on them regarding the safety of specific routes also play a critical role in safe rail operations and should be protected accordingly. In addition, since the SE application and SE service send the messages to the operations centre and RBC that may affect rail operations, this information should also be classified as Primary Assets. The authenticity and integrity of this information are particularly important. This means that it must be verifiably generated in the IoRT system and not be modified in an unauthorized manner. Further assets are software and hardware configurations such as analysis and classification methods and models, filter rules and access authorizations, as well as the software and hardware itself that support the SE functionality and are also worth protecting.

The availability, including timeliness, of SE information is necessary to ensure adequate protection against incidents. The attacker can block or delay the data sent by the IoRT sensors to the SE application or service, which in the first case prevents early warning (but can also be correctly addressed throughout the railroad system as a failure of SE functionality), and in the second case can cause damage by uncoordinated response to the delayed data due to the short response time.

Since the IoRT sensor data should not contain personal information or trade secrets, confidentiality is not prioritized as a protection goal. When using image-processing sensors, e.g., cameras, the requirements of the GDPR must be considered, so confidentiality again becomes relevant. Here, the requirements from the standard use cases (see Section 4) should be implemented. It should be noted that the SE application only requires the information that an object is on the track, further details are not necessarily required.

The architecture of the SE service provides the potential attacker with many entry points, from sensors and SE application on the gateway in the track area to the SE service in the operations centre as well as the communication links. As in the case of the PbM system, secure communication over the railroad WAN and physical protection devices in the operations centre can be assumed.

5.4 Solution

The above analysis shows that many of the standard threats to industrial control systems are also relevant to IoRT applications in the command and control domain. For this reason, the standard recommendations and IoT security guidelines of the BSI [8] and other IT security authorities should also be implemented for the investigated use cases. The study [14] analysed the applicability of various IoT security guidelines and best practices for use in the railroad sector and defined the relevant IT security requirements to protect the IoRT from cyberattacks throughout its lifecycle. The study focused on securing IoRT edge devices and communications networks rather than data centre and cloud IT security.

Accordingly, addressing the following requirements is critical to IT security:

- secure storage of secrets (credentials, cryptographic keys, etc.),
- ensuring system integrity and tampering detection,

- secure software update mechanisms,
- detection of attack attempts via the network (including (D)Dos),
- secure communication between endpoints,
- secure recovery of functionality after an attack.

The peculiarity of IoRT usage in the command and control domain is that the command and control system can be considered both as a target system for PbM and SE services and as an IoRT component itself. In addition, the IoRT sensors and gateways used by PbM and SE services must comply not only with environmental conditions but also with strict safety and security requirements to use the railroad WAN for communication, which is otherwise used only to ensure railroad operations. Another special feature is that the IoRT components, like connected command and control techniques, in the field element area are available to local attackers, who can manipulate the systems without being noticed. When using commercially available off-the-shelf products (COTS), such attacks can also be easily scale. These attack opportunities pose a challenge to the IT security of command and control systems and IoRT services alike.
In order to protect the safety-critical command and control systems against such attacks, a reference security architecture was developed within the research project HASELNUSS (haselnuss-projekt.de) of the German Federal Ministry of Education and Research (BMBF), which makes it possible to integrate necessary IT security functions into the networked command and control systems. The HASELNUSS architecture [15], [16], [17] shows how IT security functions and safety-critical applications can be implemented on the same hardware platform without interfering with each other and therefore be more tightly integrated. Until now, the implementation of these functions was strictly separated, usually also physically separated, to meet the non-interference requirements and to facilitate the safety-approval process.

The HASELNUSS reference architecture consists of a MILS (Multiple Independent Levels of Safety and Security) operating system, a hardware security module in the form of a Trusted Platform Module (TPM) 2.0 and various security services (see Figure 6).
Thanks to the data isolation and information flow control provided by the MILS operating system, a safety application (e.g. object controller, SIL 4) and security applications (with lower SIL) can be separated in such a way that they can run in completely shielded partitions on the same hardware platform without influencing each other. The usage of a TPM allows to verify remotely whether the started software corresponds to the expected configuration (e.g., the one with SIL certification) or whether it has been manipulated. The security services are executed within the dedicated security partitions and include, for example, procedures for mutual authentication between the object controller and the interlocking, monitoring of the systems integrity, secure software updates and intrusion detection system (IDS).

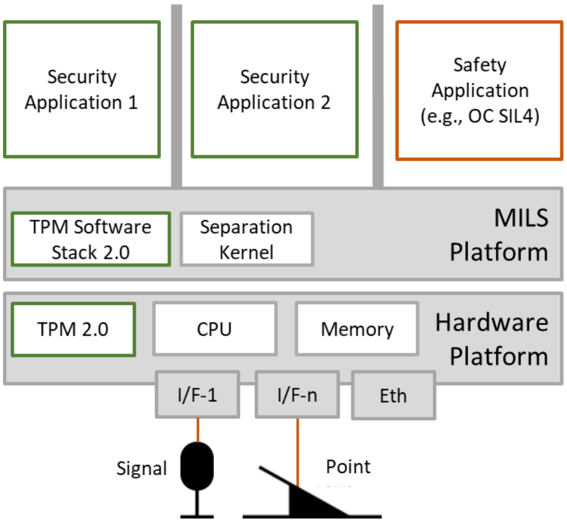

Figure 6: HASELNUSS reference architecture based on MILS platform

As part of the research project, the HASELNUSS architecture was implemented as an extension of the NeuPro architecture to protect the networked object controllers in the field element area against attacks.

On this basis, IoRT applications can also be operated both, safe and secure. In this case, the object controller can take over the functions of an IoRT gateway. The advantage is that, thanks to the HASELNUSS architecture, the same safety and security certified hardware platform is used not only for command and control, but also for IoRT applications, which simultaneously reduces the attack surface, maintenance effort, and cost. The use of specialized industrial IoRT gateways is still possible, but standard solutions based on open specifications should be preferred.

In order to map this HASELNUSS-based solution to the IoT reference architecture, certain constraints should be considered. Currently, the OC can only communicate with the systems at the DSTW level over the internal railroad WAN. In this case, safety communication (commands and signals) runs only through DSTW. The logs are stored by MDM/DOKU. In the HASELNUSS solution, the MDM also serves as a security component that forwards security alarms to the SOC and queries the state of the OC. Currently, an OC cannot be queried directly by the SOC or another service and thus can function as an IoRT gateway only to a limited extent (without Internet/cloud connection).

In the case of the HASELNUSS OC, certain edge computing functions are directly supported. For example, network packets are analysed, and security events are generated. These events are forwarded to the SOC via the MDM. In addition, the security system can perform local diagnostics and restore a secure state if necessary. The same is valid for the two IoRT applications, PbM and SE. Here, sensor data is analysed, and partially necessary responses are defined. To make this information available at higher levels, communication with the operations centre takes place.

Since the field elements currently do not support IP communication and are individually connected to the OC, an OC (safety application) can be considered as a physical device. In this case, the data is simply converted from analog to digital and vice versa and forwarded to the DSTW/MDM.

6 Conclusion

The use of sensors in a railroad operational context offers obvious advantages for optimizing process flows for the customer, for safety and for the actual operational process. This could be shown within the explanatory examples in the context of passenger stations for passenger flow control as well as security at stations and for applications in the railroad operational context for maintenance optimization.
At the same time, the highly distributed sensors with their own intelligence and their interpretation of raw data offer an extended attack surface from an IT security perspective. In the context of this studwe could ascertain that the solutions or concepts already available on the market for securing IoT devices, especially IIoT, can be suitable for establishing the necessary IT security. This is particularly true if there is no direct connection to safety related systems and correspondingly extensive approval processes.
For systems with a direct connection to railroad operations, either through relevance of the data content for operational safety or through direct communication link, new or modified approaches are necessary to meet the requirements. The information obtained with these IoRT devices is used for maintenance optimization or operational optimization and thus represents, for example, the progression of the degree of wear. If this data is altered in an unauthorized manner, failures in terms of availability but also safety-critical incidents can occur. For this reason, the integrity of the data is of particular importance. At the same time, it must be ensured that the IoRT devices can be updated or upgraded at regular intervals and can also be replaced in cycles <= 5 years to consider the corresponding innovation cycles but also, in some cases, the life expectancy of commercial off-the-shelf products. In addition to the high safety requirement, flexibility is also necessary for this.
In the solution finding process, it was determined that the IoRT devices require corresponding security gateways in order to communicate in a data-secure manner. Here, the data consumers can be the operator himself and, if necessary, also the manufacturer for maintenance or other services. Two solutions were considered. On the one hand, the integration of own security gateways, on the other hand, the data-side integration of the IoRT devices into the OT devices in the track field and use of the existing network, which is already protected from a security point of view. In the consideration it could be determined that the integration into the existing systems has the advantage that no further element has to be added in the track field and at the same time no direct Internet connection has to be established into the track field. On the one hand, this solution reduces the attack surface, and on the other hand, efficient integration can be ensured. Furthermore, from the point of view of confidentiality and privacy, the sovereignty over the disclosure of data to manufacturers or other third parties remain entirely with the operator.
The proposed solution of a MILS architecture, comparable to the solution from the HASELNUSS project, represents a possible integration solution of IoRT devices and their information into the railroad operational context. There can and will be other possible integrations. However, these should provide the following characteristics:

1. Separation of safety and security
2. Ensuring data integrity and sovereignty over data transfer for the railroad operator
3. Avoidance of direct Internet access to the track field to prevent an increase in the attack surface
4. Continuous security monitoring, for example by a SIEM or SOC, to detect attacks or misuse.

In summary, it can be stated that IoT can also offer significant added value in the railroad context. For technical integration, both Industrial IoT devices with solutions close to the standard and IoRT devices are possible. The choice depends on the area of application and the relevance for railroad operations. The decision should be made based on a sound threat analysis and subsequent risk analysis with impact analysis.

In the future, a strong increase in the use of IoT, IIoT, IoRT devices is expected. In this respect, it is recommended to develop concepts in the long term and in advance or to integrate sensor technology via IoT in ongoing IT security considerations in order to be able to ensure a harmonious overall concept. In the context of the European specification for systems close to railroad operations, fundamental consideration is given in the standardizations of EULYNX [18] and RCA [19]. A security guideline based on the prTS 50701 and IEC 62443 standards was recently developed for use in EULYNX, RCA and OCORA [20] and will be published in Q1/2021. Regardless of this, an individual consideration is always required to ensure that the country-specific threat situation as well as existing systems (legacy) are considered.

7 List of abbreviations

BMBF: Federal Ministry of Education and Research

CbM: Condition-based Maintenance

COTS: commercial off-the-shelf

(D)DoS: (Distributed) Denial of Service

DSTW: Digital interlocking system

EBA: Federal Railway Authority

ETCS: European Train Control System

FOS: Fiber Optic Sensor

GW: Gateway

IDS: Intrusion Detection System

IIoT: Industrial Internet of Things

ILS: Interlocking System

IoRT: Internet of Railway Things

IoT: Internet of Things

IT: Information Technology

LAN: Local Area Network

MA: Movement Authority

MDM: Maintenance and Data Management System

MILS: Multiple Independent Levels of Safety and Security

MitM: Man in the Middle

OC: Object Controller

OT: Operational Technology

PbM: Prediction-based Maintenance

RaSTA: Rail Safe Transport Application

RBC: Radio Block Centre (from ETCS)

SE: Situational Awareness

SIEM: Security Information and Event Management

SOC: Security Operation Centre

TMS: Traffic Management System

TPM: Trusted Platform Module

WAN: Wide Area Network

8 References

[1] DB Netz AG, „deutschebahn.com," 30 Oktober 2019. [Online]. Available: https://www.deutschebahn.com/de/presse/pressestart_zentrales_uebersicht/DB-setzt-Digitalisierungsoffensive-fort-Kuenftig-steuern-280-digitale-Stellwerke-Zugverkehr-in-Deutschland-4578022. [Zugriff am 07 Dezember 2020].

[2] BMBF, „forschung-it-sicherheit," Januar 2017. [Online]. Available: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/haselnuss. [Zugriff am 07 Dezember 2020].

[3] Bundestag, „Bundestag.de," 2012. [Online]. Available: https://www.bundestag.de/blob/192512/cfa9e76cdcf46f34a941298efa7e85c9/internet_der_dinge-data.pdf.

[4] IEEE, „IoT World forum," 2020. [Online]. Available: https://wfiot2020.iot.ieee.org/.

[5] CISCO, „CDN," 2014. [Online]. Available: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf .

[6] AG CYSIS, „Whitepaper: Security for Safety – Anforderungen an eine digitalisierte Bahnwelt," AG CYSIS, Frankfurt am Main, 2018.

[7] AG CYSIS, „Security for Safety," DVV Media Group, 2018.

[8] BSI, „Industrial Control System Security. Top 10 Bedrohungen und Gegenmaßnahmen 2019," Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019.

[9] M. Kant und D. A. Priebe, „Security for Safety," *Signal&Draht,* p. 8, Mai 2018.

[10] M. Schubert, „IT-Sicherheit im Bahnbetrieb," *Deine Bahn,* Juni 2020.

[11] C. Schlehuber, M. Heinrich, T. Vateva-Gurova, S. Katzenbeisser und N. Suri, „A Security Architecture for Railway Signalling," *International Conference on Computer Safety, Reliability and Security,* 17 August 2017.

[12] DKE, Elektrische Bahnsignalanlagen - Teil 200: Sicheres Übertragungsprotokoll RaSTA. DIN VDE V 0831-200, DKE, 2015.

[13] P. Fraga-Lamas; T. Fernández-Caramés; L. Castedo, „Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways," Basel, 2017.

[14] D. A. T. D. T. P. SNCF, „AG Cysis," Juni 2020. [Online]. Available: https://www1.deutschebahn.com/innovationsallianz/forschung/AG_CYSIS-875054.

[15] Markus Heinrich; et. al., „Security Requirements Engineering in Safety-Critical Railway Signalling Networks," in *Security and Communication Networks*, 2019.

[16] H. Birkholz; M. Zhdanova; C. Krauß; T. Arul; M. Heinrich; S. Katzenbeisser; T. Vateva-Gurova; N. Suri; D. Kuzhiyelil; C. Schlehuber, „A reference architecture for integrating safety and security applications on railway command and control systems. In International Workshop on MILS: Architecture and Assurance for Secure Systems," in *MILS@DSN 2018*, Luxembourg, 2018.

[17] C. Krauß, M. Zhdanova, M. Eckel, S. Katzenbeisser, M. Heinrich, D. Kuzhiyelil, J. Cosic und M. Drodt, „IT-Sicherheitsarchitektur für die nächste Generation der Leit- und Sicherheitstechnik," *Deine Bahn ,* 2020.

[18] EULYNX, „eulynx.eu," 2020. [Online]. Available: https://www.eulynx.eu/. [Zugriff am 07 Dezember 2020].

[19] E. ERTMS, „eulynx.eu," 07 Dezember 2018. [Online]. Available: https://eulynx.eu/index.php/documents2/press-releases/194-18c044-1-white-paper-reference-ccs-architecture-final/file. [Zugriff am 07 Dezember 2020].

[20] R. Mühlemann, „OCORA – Die europäische Initiative zur ETCS-Fahrzeugausrüstung der Zukunft," *Signal+Draht,* September 2020.

9 List of figures and tables

10 Contact and Imprint

Contact
Dr. Matthias Drodt, DB Netz AG, Mainzer Landstraße 205, 60326 Frankfurt a.M., Germany
Phone: 0049 69 265 17502 | Mail: Matthias.Drodt@deutschebahn.com

Markus Heinrich, M.Sc., TU Darmstadt, Mornewegstr. 32, 64293 Darmstadt, Germany
Phone: 0049 6151 16 25631 | Mail: heinrich@seceng.informatik.tu-darmstadt.de

The following authors of the subgroup of the CYSIS WG for IoRT - "UG IoRT" have contributed to the preparation of this white paper:

- Dr. Tolga Arul, University of Passau, Germany.
- Dr. Jasmin Cosic, DB Netz
- Dr. Matthias Drodt, DB Netz
- Marcus Friedrich, ÖBB
- Markus Heinrich, INCYDE GmbH
- Michael Kant, Consultant DB Netz
- Prof. Dr. Stefan Katzenbeisser, University of Passau
- Helmut Klarer, ÖBB
- Patrick Rauscher, DB Netz
- Max Schubert, INCYDE GmbH
- Gerhard Still, Cisco
- Detlef Wallenhorst, Cisco
- Maria Zhdanova, Fraunhofer Institute for Secure Information Technology SIT

Further information
The "Cybersecurity for Safety Critical Infrastructures - CYSIS" working group was founded on January 25, 2016 by Deutsche Bahn AG and TU Darmstadt as part of the Innovation Alliance and the existing DB Rail-Lab. The aim of the AG is to be able to effectively meet the increased challenges of cybersecurity in safety-critical infrastructures due to digitalization in the railroad sector.
The WG Cybersecurity is a basis for intensive information exchange between industry and science in the railroad sector in order to be able to benefit from mutual findings. With the help of partners from the scientific sector, including CYSEC, the profile area for cybersecurity at the TU Darmstadt, effective defense techniques and countermeasures can be researched and further developed. The desired effect is the networking of the railroad sector with academic research on cybersecurity.

Website
www.seceng.tu-darmstadt.de/cysis