# The Internet of Railway Things Security

*Whitepaper*

***Short version***

*June 2020*

SNCF

DB

TECHNISCHE UNIVERSITÄT DARMSTADT

TELECOM Paris

IP PARIS

# Contents

# 1 Introduction

This document describes cybersecurity recommendations to effectively protect Internet of Things (IoT) applications in the railway domain against cyberattacks. For this, we investigate four use cases along the railway infrastructure to study the specifics of the Internet of Railway Things (IoRT). One use case has sensors inside the train, two use cases have their sensors along the railway track and one use case has its sensors to monitor the motor of a railway level crossing. They do not describe in detail applications and services performed at the level of the data center. They rather focus on the possible infrastructures and their protection from the sensors until the data center. IoRT can be considered as a complex system comprising multiple components with an array of various important needs for security. Security is the paramount area of concern and requirements and recommendations for secure IoRT are described. A survey on various security solutions is provided. Other important requirements such as cost effectiveness, Quality of Service (QoS), and energy consumption are not addressed in this document. Based upon the four use cases, a conceptual architecture is given describing how data is transmitted and protected from sensors to data centers.

# 2 Use Cases for IoRT

We outline four families of use cases. The families cover safety-critical and non-safety-critical use cases as well as use cases from different railway operation business segments such as infrastructure and rolling stock. Subsequently, we give more details of the selected use cases that will be utilized to present the security recommendations.

## 2.1 Use Case 1: Axle Counter with Temperature Measurement

Axle counters take a paramount role in the localization of trains and therefore safe train operation. They detect which sections of the railway track are occupied by a vehicle and thus no other vehicle should be allowed to enter this section in order to avoid collisions. For this, the number of axles entering the section is counted and compared to the number of axles leaving the section subsequently.

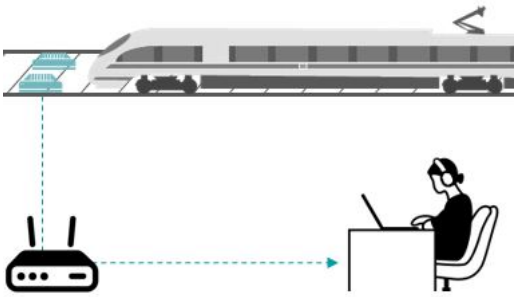

**Figure 1:** Axle counter with temperature sensor

Hot box detectors are erected at specific locations along the railway tracks. They measure the journal bearing temperatures of every train passing their location. If the temperature is above a defined threshold, the train is stopped in a subsequent station to avoid the inflammation of rolling stock, freight, or the environment due to exceeding heat and sparks.

In this IoRT use case, a large amount of axle counters are additionally equipped with temperature sensors enhancing their functional range by hot box detection. Currently, there are only around 1200 hot box detectors installed in Germany, compared to several thousands of axle counters. By increasing the number of temperature sensors, a fine-grained gradient of temperature along the train's journey is facilitated. This improves hot box detection and reduces accidents caused by overheated bearings because the trend of the temperature gradient can be used as decision criteria for stopping a train instead of a simple threshold. Combining the temperature value with the axle counter information enables the attribution of the temperature value to a single axle instead of the whole train.

Provisioning a sufficient history of temperature values for each axle allows further benefit from the gathered information for e.g. predictive maintenance purposes.

## 2.2 Use Case 2: Fibre Optic Sensing (FOS)

Fibre Optic Sensing (FOS) is used for track-side monitoring of the environment. Detection capabilities range over a multitude of applications: cable theft, landslides blocking the track, animals on track, earth fault of catenary, point machine diagnosis, flat spots of train wheels, train derailment and more. A fibre optic cable is added to the cable duct running along the railway track to enable FOS. The cable can be up to 40 km long and is connected to a detection unit located next to the cable duct. Variations in light rays are matched against a set of signatures by the sensor in the detection unit to identify preconfigured events and raise alerts.

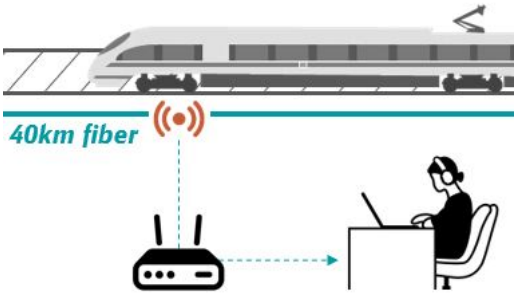


**Figure 2:** A 40 km Fiber Optic Sensing capturing the speed of a train

## 2.3 Use Case 3: Rolling Stock Remote Monitoring System

SNCF has launched an ambitious program called Télédiag with the objective of accelerating digitization and achieving radical improvement in maintenance process. Télédiag program relies on the building blocks of Industry 4.0, namely Industrial Internet of Things (IIoT), edge computing, big data, analytics and cloud computing, which allows maintenance agents to gather status information about on-board equipment in real time, providing at the same time new approaches to create a flexible production, preventive and predictive maintenance, and rolling stock remote quality control. More than 20 projects have begun, aimed at gathering through IoT information about the overall state of rolling stock equipment: door state monitoring, water level monitoring in toilet tank, on-board seat occupancy monitoring, sand-box monitoring, backup batteries state-of-charge monitoring, etc.

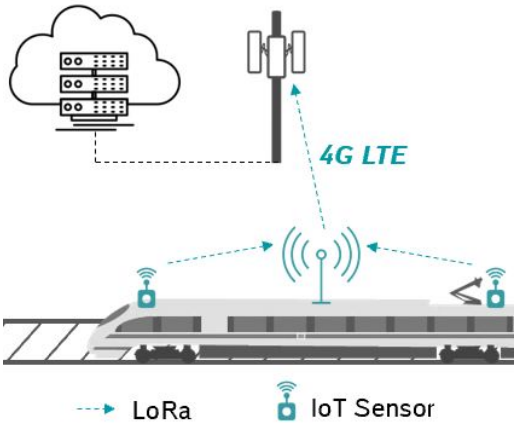


**Figure 3:** Rolling stock equipment monitoring

## 2.4 Use Case 4: Monitoring Railway Level Crossings

Level crossings are among the weakest points in railroad infrastructure seriously affecting both road and railway safety. France has over 15 300 railway level crossings (however, there is no level crossing along high speed train lines). According to the European Union Agency for Railways (ERA), every year in Europe, more than 330 people are killed in more than 1200 accidents at railway level crossings[1]. Thus, high level of safety is required for any rail level crossing.

[1] https://trimis.ec.europa.eu/project/safer-european-level-crossing-appraisal-and-technology

The goal of this use case is to monitor the "open-closed" state of the level crossing barrier with two targets. Not only will it detect the functioning of the barrier but it will also detect shock with any vehicle. This can be done using an IoT system which remotely reports irregular electrical signals observed on the motors of the barrier to the network control center or directly to the train driver.

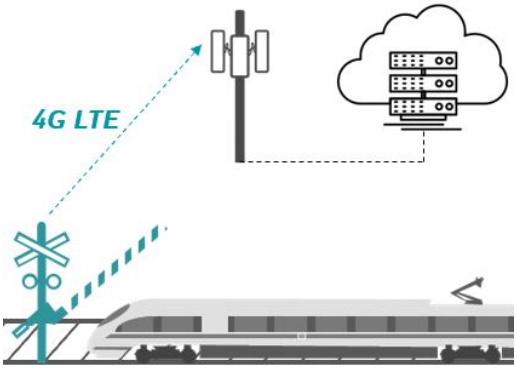


**Figure 4:** Railway level crossing

### 2.5 Conclusions from the Use Cases

Having described the four use cases from various applications in the railway domain, we now summarize the lessons that can be learned from the use cases. A striking commonality between the use cases is the location of their deployment in a comparatively hostile environment from a security perspective. Some of the IoT devices are deployed in an area that is easily or frequently accessible by an uncontrollable group of people interacting with the transportation system (using a train, using a level crossing). All edge devices' locations require sophisticated protection against physical attacks as they are hard to supervise them somehow to discover possible attackers. We even have sensors at hand that constantly change their location as they are mounted on a train, which is quite unique to the transportation sector. It is also important to highlight that an attack on some critical sensors could lead to severe damage, human injury or even death, which emphasizes the necessity to carefully deal with cybersecurity in the IoRT. Railway transportation is characterized by the long lifetime of some components like trains and tracks that is in the range of several years to decades. Thus, applying IoRT sensors to legacy hardware has to be considered as well as IoRT devices being replaced with newer hardware during the lifetime of the monitored use case.
All in all, it is important to protect the IoRT system sufficiently from physical tampering and to ensure that the collected information is transmitted securely to the data center supported by a number of communication protocols depending on the chosen type of transmission. Security in this context demands to protect the IoRT system's authenticity (implying integrity), confidentiality, and availability. We will discuss how this can be achieved in the following section before we present a generalized security reference architecture to structure communication and security in the IoRT.

## 3 Recommendations for a Secure IoRT

After carefully studying the use cases, we discuss security requirements to protect the IoRT from cyberattacks. We focus on securing IoRT edge devices and communication networks and less on the security of data centers and the cloud.
The requirements chapter is structured along the IoRT lifecycle which is presented in the following section, before device and network requirements are discussed.

### 3.1 IoRT Lifecycle

The railway IoT security requirements for devices in Section 3.2 and networks in Section 3.3 are structured along the IoRT lifecycle shown in Fig. 5. The lifecycle comprises the five phases *provisioning*, *deployment*, *operation*, *update*, and *decommission*. We explain the five phases in the following paragraphs.

**Provisioning** While designing, creating specification sheets, and ordering IoRT equipment, the foundation of a proper security concept is laid. The components must meet the security requirements of later phases, because hardware cannot be changed easily and inexpensively, once acquired.

**Deployment** IoRT equipment must be installed properly to be secure. To ensure security, several components might require one time actions like changing default access credentials and creating a fresh digital identity.

**Operation** The operation phase is the longest and thus most important phase in a security lifecycle as well as the phase where the system is the most exposed to threats. Depending on the railway IoT system's functional requirements, the length of the operation phase can range from a few days to several decades. The provisioning and deployment phase prepare the system for secure operation. Still, secure operation must be closely monitored to successfully defend against attacks.

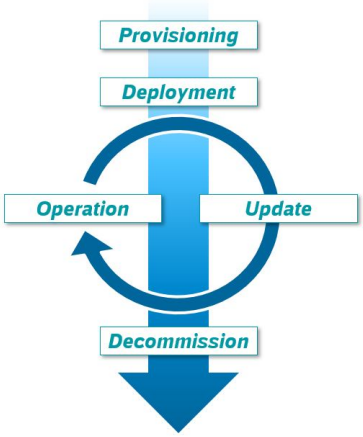


**Figure 5:** IoRT Lifecycle

**Update** A fundamental insight into security is that security is a process. The threat landscape of information technology (IT) and operational technology (OT) security is ever changing and an arms race of attackers versus defenders. Every system and IoRT systems in particular need to be updated and brought to the state-of-the-art frequently to maintain a sufficient security level. It is important that functional as well as security updates are performed in a secure manner without introducing weaknesses to the system. Once a vulnerability is discovered in an operational system, an update is prepared and the system switches to the update phase. After a successful, secure update, the system returns to the operation phase.

**Decommission** At the end of a component's lifetime, security must be considered as well. The component might be disposed or sold and re-used elsewhere after its mission in the IoRT. In any case, the component must experience proper security treatment such that the security concept and the protection measures of remaining components is not weakened.

## 3.2 Security for IoRT Devices

This section focuses on requirements and recommendations for IoRT devices.

### 3.2.1 Provisioning

**Hardware Security** Edge devices utilized in a railway application are likely to be deployed in an open, accessible, and unprotected environment. Adversaries might easily gain physical access to one or many devices of the IoRT. To protect confidential data like cryptographic keys, the hardware should also provide some sort of secure storage from which data can not be extracted by unauthorized persons. Secure storage can be provided by technologies like Trusted Plattform Module (TPM), Trusted Execution Environment (TEE), and hardware security module (HSM). Many cryptographic security applications rely on random numbers. A secure cryptographic random number generator can already be provisioned in hardware if necessary.

**Resources for Security** Processor, memory, and storage of an edge device should be configured strong enough to handle the intended application and additionally, adequate security functionality to protect the system. Without being considered in the provision phase of a system, constrained IoRT devices are likely unable to host security applications.

**Reserve Resources for Updates** The system resources should provide sufficient margins for updates. A durable system should be equipped with additional resources to accommodate for future resource demands. The resources mainly concern the processor, memory, and persistent storage.

**Manufacturer Provides Updates and Support** Up-to-date devices is a prominent aspect of a profound security concept. The operator of an IoRT should ensure that device manufacturers provide software updates for closing vulnerabilities over the whole lifetime of the product and spare parts are available if needed. This should be regarded during provisioning while selecting a manufacturer and ordering the devices.

**Product Security Certification** During the provisioning process, attention should be paid that hardware is certified according to domain security standards if possible. Certification should establish trust in the manufacturer, that the product has been developed and build with high security standards. Popular security certification is provided by the ISO 27000 standard series, the IEC 62443 standard series, or the IACS Cybersecurity Certification Framework [15].

### 3.2.2 Deployment

**Remove or Change Default Credentials** Many commercial off-the-shelf (COTS) devices are shipped with default passwords or default credentials intended for setting up the device. Unfortunately, default credentials can often be easily obtained from the Internet. Thus, during the setup of a IoRT system and the addition of new device, it must be ensured that no default passwords, credentials, and accounts are left on the devices. They can be changed to unique credentials or fully deactivated while other accounts are used for operation and maintenance.

**Unique Credentials per Device** Access credentials should be unique per device.

**Remove or Block Unnecessary Physical Interfaces** Unnecessary or unused interfaces to the edge devices should be disabled or blocked to prevent misuse and intrusion. Modern devices are shipped with a variety of physical interfaces, including USB ports, Ethernet ports, fibre channel ports, other wired networking ports, and card readers. Less visible but similar widespread are wireless interfaces: Wi-Fi, Bluetooth, ZigBee, Cellular (GSM, GPRS, UMTS, Long-Term Evolution (LTE), 5G), and more. For stronger protection that simply deactivating, unnecessary physical interfaces can be sealed with resin, protected with locks, or even desoldered from the circuit board.

**Disable Unnecessary Services** Similar to the deactivation of unnecessary physical interfaces, unnecessary services should be deactivated or removed from an IoRT device to reduce the attack surface. Open ports reveal active services of which only allowed services should be running and able to communicate with other devices.
Where services cannot be disabled, respective firewall rules should be established to block all communication from and to the services interface on the device.

**Secure Interfaces, APIs and Services** Complementary to disabling unnecessary services, the required services of the devices should be minimized to the level required for operation. Debugging tools, setup routines and other software required for device installation but not required for operation should be disabled after installation.

### 3.2.3 Operation

**Logging** IoRT devices should implement a logging system that records events related to user authentication such as successful and failed logins as well as remote access. Management of accounts and access rights, modifications to security rules, and the functioning of the system should be logged as well. The logs should be preserved on durable storage that persists data without power supply, because IoT devices can run on battery that can go empty.
When saved on edge devices or a logging server, logs should be protected from unauthorized changes to prevent disguising incidents in any case.

**Strong Mutual Authentication** Edge devices as well as fog and cloud devices should be able to perform strong mutual authentication for every interaction. Authentication is necessary to ensure that data flow is only established between licit devices and cannot be manipulated by an attacker. Interactions include the transmission of measured data by sensors, commands to actuators as well as firm- and software updates and configuration changes. For each type of data modification, there are a multitude of attack scenarios how an attacker can profit from manipulating data. Therefore, device as well as user authentication is required for security.
Passwords should follow a password policy that describes passwords which are not easy to guess by a dictionary attack, sufficiently long to endure a brute-force attack.
The German Federal Office for Information Security (BSI) regularly publishes "Cryptographic Mechanisms: Recommendations and Key Lengths" [5].
To further strengthen authentication, multiple authentication types can be combined to two factor authentication (2FA) or multi-factor authentication (MFA).

**Secure Storage for Credentials** Authentication credentials should never be stored in plain text on any devices. This is especially true in an open and weakly protected environment like IoRT. Compared to physically protected devices, chances are high that an IoRT device is stolen which enables offline attacks that are virtually unlimited in computing power and time. Again, a reason why credentials should be unique per device.

**Secure Storage for Data** Similar to credentials, other sensitive or confidential data on edge devices should reside in encrypted storage [1]. This includes user information, facility information, collected data like sensor readings, camera footage, as well as production data, like configuration or models of machine learning algorithms.

**Authorization** Edge devices should employ an authorization model for actions to perform, data access and code to execute. Privileged code e.g. to perform software updates should be isolated and not executable by the same user as e.g. the measurement process of a sensor or the control process of an actuator. Data should only be readable and writeable by necessary executables. This prevents an attacker from further reading and modifying code and date from a compromised process.

**Accountability and Non-Repudiation** In an IoRT environment with multiple stakeholders, users and numerous devices, attribution of actions and data is important. Depending on the use case accountability and non-repudiation can be security goals, which can be achieved with digital signatures.

**Safety and Reliability** IoRT edge devices are exposed to tough environmental conditions such as varying temperature and humidity.
While environmental conditions are an issue of reliability in general, great care needs to be taken to protect the system's safety to avoid consequences like damage, loss, injury, or even death.
It is important to understand the consequences of the interruptions and prepare respective fail-safe and fail-secure countermeasures. It should be considered as well that an attacker could also provoke the listed interruptions to perform an attack.

**Input Validation and Data Authentication** A common entry point for malware and exploits are insecure application programming interfaces (APIs) provided by a device. Data originating from other devices or even other software components on the same device should not be trusted without further measures.
For enhanced security, all data transmitted should be authenticated. Message authentication codes (MAC) or digital signatures can be attached to the data to provide authenticity and increase the trust in the information. A MAC is based on a pre-shared secret between sender and receiver while digital signatures rely on a public key infrastructure (PKI) and asymmetric cryptography.

**DoS Protection** APIs exposed to the network can be subject to denial-of-service (DoS) attacks that flood the API with too many requests to handle for the device. Such attacks can be mitigated by rate-limiting the API access to an amount that the device is able to process or by implementing a load-balancing infrastructure to distribute the requests to multiple devices. [4].
In general, an IoRT device should be able to deal with interrupted connections, whether they are cable connections or wireless. The connection could be interrupted accidentally or intentionally by an attacker. Countermeasures include redundant connections and the ability for the device to buffer data to be send in order to retry once the connection becomes available again to avoid data loss. Most importantly, the connection to an edge device should be monitored constantly for immediate reaction on a loss of service.
Wireless connections as they appear in our use cases (Long Range (LoRa), 3G, 4G, LTE) are prone to DoS attacks. An attacker can jam the transmission frequencies with a jammer that can readily be bought off the Internet for less than 1000 $. Currently, there is no solution available to fully defend against jamming attacks. Jamming detectors can be utilized to identify offenders and increase their change to be discovered. Redundancy in connections or cable connections can be used as a defence strategy [7].

**Malware Protection** The two most common ways for malware to infect devices are via removable media such as USB flash drives and notebook computers as well as via a network connection [7]. But also APIs could be exploited to load malware on an IoT device [1].
Maintenance devices such as notebook computers should be regularly scanned for malware with an up-to-date virus scanner. In our use cases, a regular virus scan on the edge devices is not applicable due to limited resources. However, scans on the edge device are not necessary if other countermeasures apply. One approach is to only allow the execution of whitelisted binaries on the edge devices [3] such that malware is not executed even if it finds its way on the device. The communication network should be segmented from other networks, either physically or virtually with the help of a Virtual Private Network (VPN) [7]. Also an intrusion detection system (IDS) could be employed, either on the device or, if device resources are limited, on the network to monitor anomalous behaviour and raise alerts.
Removable media (e.g. USB flash drives) should be subject to strong controls such as whitelisting, device personalization, exclusive use, and encryption [7]. With removable media, even "airgapped" systems (i.e. systems without network connection) could be infected with malware. The most infamous example being Stuxnet.

**Identity Revocation and Exclusion of Devices** The IoRT system should provide a mechanism to exclude edge devices from participation. Reasons to enable this mechanism could be that the device is malfunctioning (sending bogus data), a vulnerability became known (exclude the device as a precaution), or the device is known to be compromised.

**Backup** In case of failure, misconfiguration or a compromise it might be necessary to restore an IoRT device. To be able to do this, it is necessary to provision backups of configuration files and data. Backups should be created automatically on a regular schedule. In some cases, configuration of edge devices is managed from a central server and all collected data is not stored on the edge device itself. Then, a backup might not be necessary as the configuration can be re-deployed to the device from the server. If the backup contains sensitive information, encryption should be employed for the backup.

**Secure Communication** Although secure communications is a property for networks, the edge devices must support network security as well. This includes the support of Transport Layer Security (TLS) [4, 6, 7], VPN [6], and secure shell (SSH) [6].

**Security Testing** Similar to safety validation, the security properties of a system can and should undergo a variety of tests to evaluate their performance. An extensive list of possible security tests is given in annex C of European Union Agency for Cybersecurity (ENISA)'s publication [3]. The most important tests are static analysis security testing, dynamic analysis security testing, fuzzing test and penetration testing.

### 3.2.4 Update

**Asset and Configuration Management** Three of our use cases describe a comparatively homogeneous system with only one type of IoT sensor. However, the rolling stock monitoring use case (see Section 2.3) comprises a variety of different sensor types (i.e. edge devices). On top of that, the sensors are mounted on a train and thus are constantly changing their physical location. For managing the diversity in hard- and software, it is important to maintain a database of all the assets including their hardware version, versions of important software and applications, their digital identity (e.g. a digital certificate), and their location. Thereby, affected devices can be quickly identified in case an update is required, e.g. because a software vulnerability became known.

**Monitor Asset Vulnerabilities** Active monitoring of the assets security vulnerabilities should be performed to be alert of a vulnerability as fast as possible, such that an adequate reaction can be dispatched in time. Vulnerabilities of a variety of cybersecurity-related products and services are collected in databases such as CVE[2].

**Secure Update** Edge devices should facilitate the possibility to update their firm- and software to roll-out new functionality and to patch security vulnerabilities. Unpatched systems are left vulnerable to attacks. Such an update should be performed in a secure manner so that it does not constitute an additional attack surface. ENISA recommends that updates can be performed over-the-air, the connection used to transmit the update is secure, that the update does not contain sensitive data, and that the update is digitally signed to be verified by the updated device [4].

[2] `https://cve.mitre.org/`

### 3.2.5 Decommission

**Sanitize Device** Once a device reaches its end of use a proper decommission is required to not put the remaining system and business at a security risk. Devices could be decommissioned as well because they reached their end of life or they will not longer be used because they were compromised. Decommissioned devices are typically trashed or can be sold to be re-used somewhere else.
In all cases critical data for operation and security needs to be removed from the device. Security data comprises digital identities, device passwords, service credentials, confidential operational data, logs, and network access credentials (e.g. Wi-Fi passwords).
For sanitizing the devices, they could be equipped with a reset mechanism that clears all sensitive data and restores the device to factory settings [1] what makes them quickly available for re-use. The National Institute of Standards and Technology (NIST) published a detailed guide for sanitization of a device's storage media including detailed information how hard drives, solid state drives, and flash drives can be securely treated depending on their security classification [10]. This process however goes beyond removing sensitive data by erasing all memory which renders the device unusable until a new firmware or operating system is installed. Depending on the edge device and the sensitivity of the data, erasing the whole memory might be disproportional. A checklist should be maintained where sensitive data is stored that can be used during sanitization of the device [6].

**Remove Data Traces from other Devices** In the connected world of IoT, a device will leave many data traces on other systems as well. From a security perspective it is important to control those traces as well. The most important task is to revoke the decommissioned device's digital identity, e.g. its digital certificate within a PKI. But most likely there are more traces to be taken care of, to name a few: DHCP leases for IP address assignment, entries in whitelists to, e.g. allow communication, firewall rules for the device, and entries in asset management databases.

## 3.3 Security for IoRT Networks

This section focuses on requirements and recommendations for IoRT networks.

### 3.3.1 Provisioning

**Security architecture** The diversity of IoT applications makes it vulnerable to malicious actions. Thus, the number of devices is also a challenge for the security of the IoRT. In particular, we must ensure while creating specification sheets (1) a strong design of an end-to-end security protocol, (2) an integration of a one time password mechanism for device authentication and (3) a formal analysis of the proposed protocol.

**Network and Security Equipment's Certification** During the provisioning process, attention should be paid that the firewalls and security equipment such as VPN client, IDS, Intrusion Prevention System (IPS), etc. are certified according to a national security agency such as Agence nationale de la sécurité des systèmes d'information (ANSSI) in France or the BSI in Germany. Certification of equipment is a proof of a product's robustness, based on a compliance analysis and penetration tests performed by an evaluator.

**Standards and Technologies** During the provisioning process, attention should be paid to the standards and the technologies used in the IoRT. In fact, the deployment of IoT needs communication standards that seamlessly operate among the various objects. Several worldwide organizations are involved in standardizing such communications. These include the International Telecommunication Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE), the Internet

Engineering Task Force (IETF), Global Standard1 (GS1), the Organization for the Advancement of Structured Information Standards (OASIS), the Industrial Internet Consortium (IIC), and several others.

### 3.3.2 Deployment

**Firewall Deployment** Firewalls are key elements for the overall security architecture in the IoRT. A firewall provides critical filtering functionality for network traffic. Different firewalls equipment's are needed in the IoRT: inside the train and in any network where we have devices. There are different types of firewalls: packet filters and application layer for more protection for critical systems. A packet filter firewall is primordial because the IoRT is exposed to different types of attacks. In the deployment process, firewalls should not be over-deployed because multiple firewalls usually increase security levels and decrease the performance. Firewalls should be deployed to make zones of authorized traffic, separating applications into sets of related security requirements.

**Intrusion Detection System** An IDS can be a significant element of the network security strategy. Deployment of such security device is of great importance. An IDS compares activities with attack signatures, which are sets of characteristic features of an attack or its pattern. IoT is highly vulnerable to attacks for numerous reasons: (1) usually, devices spend most of the time unattended, and they are therefore fairly easy to be attacked physically, (2) most of the communications are wireless, which enables Man-in-the-Middle attacks, one of the most common attacks on such a system. Consequently, exchanged messages may be subject to eavesdropping, malicious routing, message tampering and other attacks which affect the security of the entire IoRT system, and (3) multiple types of objects have limited resources in terms of energy and computation power, which prevent them from implementing advanced security solutions.
In IoRT, an IDS can monitor network traffic for these attacks and suspicious activities and issues alerts when such activities are discovered.

**VPN Tunnelling** A Virtual Private Network (VPN) is a secure private network connection across a public network. In IoRT, VPNs can be used to connect the local network on a train across the Internet with a remote gateway at the network of the data center. A VPN tunnel ensures the data confidentiality, data integrity and equipment's authentication. There are different tunnelling protocols to be used. However, an Internet Protocol Security (IPsec) one is recommended between two networks. On the other hand, TLS provides a secure VPN connection between remote devices and the data center or any other servers on the network.

**Segmentation Policy** Attention should be paid to controlling how traffic flows among the different network segments. This operation is called segmentation and it is used in order to enhance the performance and to ensure security. The segmentation can be done by filtering all traffic in one segment from reaching another, or limiting the flow by traffic type, source, destination, and many other options. This filtering can be done by firewalls rules.

**SIEM Security Information and Event Management** A security information and event management (SIEM) solution allows the analysis of security events in real time. A SIEM platform allows to monitor applications, user behaviors and data access. It is therefore possible to collect, normalize, aggregate, correlate, and analyse event data from equipment, systems and applications (firewall, IDS/IPS, network machines, security machines, applications, databases, servers, directories, IAM). There are many SIEMs that can be used such as Splunk, OSSEC, IBM QRadar, ArcSight, etc.

**Activate Secure Protocols** On any device or server only the version TLS 1.3 should be used. This version is highly secure and lightweight. As for datagram transport layer security (DTLS), only the version DTLS 1.2 should be used.

**Protected Network** When configuring the network, attention should be paid that there is no back door access to the protected network. A gateway or access point must be appropriately protected with password and encryption. On the other hand, direct access to network equipment should be prohibited for unauthorized personnel.

### 3.3.3 Operation

**Authentication** Authentication is the process of verifying the identity of a device by obtaining some sort of credentials and using those credentials to verify the device's identity. In railways networks, authentication and authorization are required to determine assigned roles to entities and their allowed actions within the system (what types of messages can be sent, what applications can be accessed, and what functions can be executed). There are multiples authentication schemes in IoT:

- Mutual authentication schemes
- Two party authentication through a trusted party with key exchange
- Session key based authentication
- Group authentication
- Directed Path based Authentication Scheme (DPAS)
- one-time password (OTP) and SecureID Authentication Schemes

The majority of the schemes are dependent on the specific architecture of the IoT system.

**Availability** Availability refers to ensuring that only authorized parties are able to access the information and functions when needed. In an IoRT system, availability is required to enable safety applications and other services to remain operational even in the presence of an incident. This service could be provided by server redundancy and the High Availability (HA) service.

**Integrity** Integrity of information refers to protecting information from being modified by unauthorized parties. In an IoRT system, integrity is ensuring the non-alteration of messages exchanged between different sensors.

**Confidentiality** Confidentiality of information is protecting the information from disclosure to unauthorized parties. In an IoRT system, some applications and messages should be accessible only by authorized parties, since exchanged data within these messages is considered confidential. Using recommended cryptographic cipher suites and an efficient security strategy can ensure this security service.

**Accountability and Non-Repudiation** Accountability refers to the possibility of tracing actions and events back in time to the users, systems, or processes that performed them, to establish responsibility for actions or omissions. Non-repudiation refers to the ability to ensure that a party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. In an IoRT system, accountability and non-repudiation are essential security requirements especially when accidents or errors occur as a result of sending wrong information.

**Secure Communication** From a cybersecurity point of view, creating a secure transmission channel can be implemented at different levels in IoT: network/link layer, transport layer or application layer. Implementing the classical communication security protocols and cryptography functions in an IoRT system is limited by the resource capabilities on the used objects. In railway networks, the limited capabilities of a resource can be mitigated by using lightweight protocols or adapted version of the security protocols. The layers in an IoT stack are very similar to that of the IP model but there are few differences among the layers. For example, TLS and DTLS protocols are usually used above the transport layer. The constrained application protocol (CoAP), Message Queuing Telemetry Transport (MQTT), XMPP and several other protocols are used across the application layer with a security protocol.

### 3.3.4 Update

**Risk Analysis** Risk analysis is part of a comprehensive risk management process. It has a legal, security and human dimension. Risk analysis is the process of identifying threats on networks, analysing or evaluating the risks associated with a threat, and determining the appropriate means to eliminate, control, or correct these risks. An equipment or device update could be based on the risk analysis following the detection of an obsolete version in an equipment or a bad configuration.

**Secure Update** The more regular the updates are, the more the supervision meets efficiency requirements by allowing the integration of new equipment and protocols. Having an up-to-date version meets the constraints of cybersecurity and actively participates in the security of the IoRT devices and equipment such as IDS, VPN and servers. The best way is to have the new versions available as regularly as the manufacturer makes them available. The software maintenance contract, including free access to any new version, is the surest way to keep the supervision up-to-date. To ensure that no unauthorized release of information from the isolated network can occur, a secure update solution can be further reinforced by performing anti-virus checks on the incoming updates. A secure update solution must accomplish a timely and efficient automated transfer whereas ensuring that no data can leave the network, thus preserving confidentiality.

### 3.3.5 Decommission

**Backups** Before any erasure or destruction operation, it is recommended to check that the device or equipment does not contain any useful data that is not otherwise backed up. If this is not the case, a data backup is necessary.

**Sanitize Device** The destruction of used or damaged equipment or device is an operation that requires special precautions and adapted equipment. The lifecycle of equipment (reassigning equipment internally, sending equipment for maintenance, selling equipment, etc.) can lead a third party to access this equipment and the data it contains. It is essential to prevent the leakage and exploitation of such data by securely erasing it or destroying the storage medium before putting it in the hands of a third party.

**Safely Discard the Old Equipment** Old equipment should be safely trashed while maintaining data confidentiality and respecting the environment.

# 4 Reference Architecture

The majority of the described use cases have some commonalities: all of them are collecting data in order to be processed in a data center, particularly for predictive maintenance purposes. Most of them are outdoor with components accessible to the public (be passengers or passing-byes).

This is stressing the need for tamper resistance or resilience of the exposed sensors: resilience with regard to both environmental conditions and human tampering. All use cases must be developed in a cost effective manner since they are deployed along a large network of railway tracks or within numerous rolling stocks. They may be deployed progressively one or several elements at a time depending for instance upon the readiness of operational crews and the criticality of a section of railway track or a level crossing. Always with respect to security requirements as described in Section 3.2 and Section 3.3. This progressiveness appears to be an important property of a very large network such as the railway network, as it allows avoiding an overall rollout that is always extremely complex and even risky when it is about deploying new technology like IoRT.

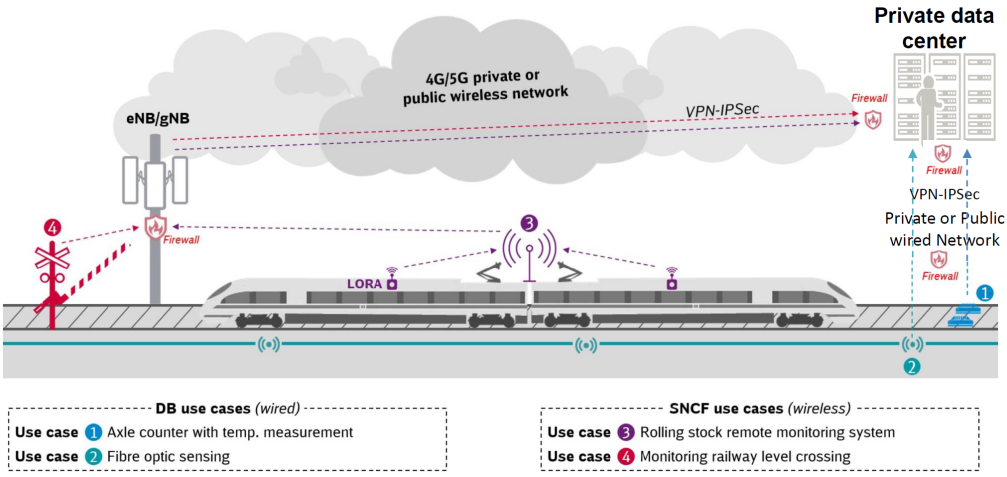


**Figure 6:** Reference Architecture Global View. The four use cases are presented along the same railway track with a common data center, and two modes of communication: wired and wireless. eNB and gNB stand for base station, eNB (for evolved node B) interfaces with GSM or LTE while gNB (for next generation node B) interfaces with 5G. Message protection by VPN and IPsec have been seen in Section 3.3.2.

The communication can be separated in two layers: a private one which is close to the sensor layer. This layer can perform edge computing, to optimize latency but also to prepare data to be transmitted (aggregation, cleaning, filtering). We can assume high trust in equipment located in the private layer as it is typically under the control of the IoRT operator itself. The second layer can go through the public network to communicate data towards data centers in a cost effective manner. Again, this may impact the real time requirements such as the ones described in use case 4 in Section 2.4. For example, if the train conductor must take quick emergency measures when an alert is detected. It can be extremely interesting to be able to deal with this type of outlying behavior at the level of the private second layer (the "edge") before entering in the public network. Data passing through the public network will most likely be protected by the public network operator. This must not prevent the railway operator to perform their own data protection as otherwise a high level of trust is put in the network operator which is hard to ensure. Thus, it is recommended to install data protection services (including but not limited to firewalls and encryption) at strategic nodes of the IoRT architecture, in particular before the entry into the public network, or at the entrance of the data center. Firewalls are installed at the entry and the exit of the different layers separating them from one another, protecting the network from intrusion and enforcing the access policy designed by the railway operator. Firewalls can be more or less complex according to the criticality of the application and the intelligence required by the access policy.

The reference architecture is dealing with a secured data flow from the sensor to the data center and focuses mostly on the measurement data flow from the sensors towards the IoRT data center where it can be further processed and create value for the railway company. The security architecture is the same throughout the use cases. The topology of the network must be understood at a conceptual level rather than at an actual level. It covers both wired and wireless technologies. In the real world, the physical network will be more complex and communication protocol stacks may differ according to required QoS and performance. There must exist several redundant routes to go from one point to another in order to avoid single point of failure. There may be several data centers involved (public and private).

# 5 Vision and Conclusion

We conclude in two steps. First, we reaffirm the importance of the IoRT that is essential to the viability of the railway system of today and the great innovations awaited for tomorrow. Second, we must never forget to treat cybersecurity truly inseparably to the operation of any IoRT system. Smart sensors have progressed at an extremely rapid pace in a couple of years and are being deployed in all kind of industries. IoRT is offering the railway industry an unprecedented continuous surveillance of various critical devices both along the railway tracks and in the rolling stock. It is greatly improving security, traffic, and passenger experience at the same time. One beneficial property from the reference architecture that has been proposed is, that it will allow to develop other applications in the future than the ones described in the four use cases of this whitepaper. The communication infrastructure and connectivity will be completely re-usable and a new application would be deployed at the sole cost of installing new sensors along the railroad and to develop new software. Data protection will follow the same methods as well.
Combined with edge computing, IoRT reduces latency, increases security and safety, and will allow the data center to deal with less data for the same expected results. It will also allow to rapidly send alerts. Combined with artificial intelligence (AI), IoRT is a key enabler for innovative and effective predictive maintenance applications.
To deliver the autonomous train of the future, it will be mandatory to increase the security level for a number of devices due to the simple fact that the human train driver has been replaced by a machine that could not be able to properly handle unpredictable events. This will not be possible without IoRT in full deployment providing alerts in critical real time thanks to edge computing.
To deliver multi-modal transportation in the future it will be mandatory to increase the dialog between passengers and intelligent data centers, always owning the most recent data about the traffic. Of course, AI algorithms, and smart contracts from blockchains will have an important role, but first, IoRT will have to be in full deployment to collect required data.

**Next Generation Railway Cybersecurity** Due to the increasing number of IoRT devices expected in the future, their management will become an important and complex task from a cybersecurity perspective. Keeping track of the status of the numerous IoRT assets as described in Section 3.2 can be challenging because of the spatial distribution over a whole country (or even more). On top of that, some of the assets are changing their location frequently so that it is hard to determine their current location or predict their location in the future if for example maintenance access is required. Especially devices attached to freight cars exhibit complex movement patterns. As part of the asset management, the identity management needs to be efficient and fast in the face of the number of devices. We assume cryptographic certificates and a PKI to constitute device identities. Identifying which devices are compromised, revoking their identities in consequence, and distributing this information to all necessary identities can be cumbersome. It is crucial to monitor all identities to quickly identify compromised ones. Particularly with moving devices, a remote connection to the PKI can not be guaranteed while a benign device might already have contact and exchange data with a compromised and actually revoked identity.

Physical protection has been identified as a key property of IoRT security that will become a prominent task in the use cases and other future IoRT applications. It is closely tied to identifying compromised devices as this is the second line of defence if a device cannot be protected properly against physical attacks or an attacker overcomes the protection.
The expected increasing machine to machine (M2M) communication triggers actions in the railway system without involving human intervention. This demands proper security supervision and abilities for intervention to detect and react to misuse and attacks.
It seems a daunting task to deploy next-generation cybersecurity on a full existing railway system, however, it is a task no administration or serious railway business can afford to ignore.

# Acronyms

| | |
|---|---|
| **2FA** | two factor authentication |
| **AI** | artificial intelligence |
| **ANSSI** | Agence nationale de la sécurité des systèmes d'information |
| **API** | application programming interface |
| **BSI** | German Federal Office for Information Security |
| **CoAP** | constrained application protocol |
| **COTS** | commercial off-the-shelf |
| **DoS** | denial-of-service |
| **DPAS** | Directed Path based Authentication Scheme |
| **DTLS** | datagram transport layer security |
| **ENISA** | European Union Agency for Cybersecurity |
| **ERA** | European Union Agency for Railways |
| **FOS** | fiber optic sensing |
| **HSM** | hardware security module |
| **IDS** | intrusion detection system |
| **IIC** | Industrial Internet Consortium |
| **IIoT** | Industrial Internet of Things |
| **IoRT** | Internet of Railway Things |
| **IoT** | Internet of Things |
| **IPsec** | Internet Protocol Security |
| **IPS** | Intrusion Prevention System |
| **IT** | information technology |
| **LoRa** | Long Range |
| **LTE** | Long-Term Evolution |
| **M2M** | machine to machine |
| **MAC** | message authentication code |
| **MFA** | multi-factor authentication |
| **MQTT** | Message Queuing Telemetry Transport |
| **NIST** | National Institute of Standards and Technology |
| **OTP** | one-time password |
| **OT** | operational technology |
| **PKI** | public key infrastructure |
| **QoS** | Quality of Service |
| **SIEM** | security information and event management |
| **SSH** | secure shell |
| **TEE** | Trusted Execution Environment |
| **TLS** | Transport Layer Security |
| **TPM** | Trusted Plattform Module |
| **VPN** | Virtual Private Network |

# List of Figures

# List of Tables

# Bibliography

[1] Fred Baker et al. Internet of Things (IoT) Security and Privacy Recommendations. Technical report, Broadband Internet Technical Advisory Group, 2016. URL https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php.

[2] ETSI. TS 103 645: Cyber Security for Consumer Internet of Things. Technical report, ETSI, 2019. URL https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.

[3] European Union Agency for Cybersecurity. Good Practices for Security of IoT. Technical report, ENISA, 2019. URL https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1.

[4] European Union Agency for Cybersecurity. ENISA Good practices for IoT and Smart Infrastructures Tool, 2019. URL https://www.enisa.europa.eu/iot-tool.

[5] German Federal Office for Information Security. Cryptographic Mechanisms: Recommendations and Key Lengths. Technical report, BSI, 2019. URL https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html.

[6] German Federal Office for Information Security. IT Baseline Protection: SYS 4.4 General IoT Device, 2019. URL https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_4_Allgemeines_IoT-Gerät.html.

[7] German Federal Office for Information Security. Industrial Control System Security Top 10 Threats and Countermeasures 2019. Technical report, BSI, 2019. URL https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005E.html.

[8] GSM Association. CLP.13 – IoT Security Guidelines for IoT Endpoint Ecosystem. Technical report, GSMA, 2017. URL https://www.gsma.com/iot/iot-security/iot-security-guidelines/.

[9] Daniel Miessler, Aaron Guzman, Vishruta Rudresh, and Craig Smith. Owasp internet of things top 10. *OWASP Foundation*, 2018. URL https://owasp.org/www-project-internet-of-things/.

[10] National Institute of Standards and Technology (NIST). Guidelines for media sanitization. *Special Publication (NIST SP)-800-88*, 2014. doi: 10.6028/NIST.SP.800-88r1. URL http://dx.doi.org/10.6028/NIST.SP.800-88r1.

[11] National Institute of Standards and Technology (NIST). Digital identity guidelines authentication and lifecycle management. *Special Publication (NIST SP)-800-63B*, 2017. doi: 10.6028/NIST.SP.800-63b. URL https://doi.org/10.6028/NIST.SP.800-63b.

[12] National Institute of Standards and Technology (NIST) and United States of America. Framework for improving critical infrastructure cybersecurity. Technical report, NIST, 2018. URL https://doi.org/10.6028/NIST.CSWP.04162018.

[13] Project Group End2End Security Smart Metering. Requirements Catalog End-to-End Security for Smart Metering. Technical report, Oesterreichs Energie, 2014. URL https://oesterreichsenergie.at/sicherheitsanforderungen-fuer-smart-meter.html.

[14] Sven Schrecker, H Soroush, J Molina, J LeBlanc, F Hirsch, M Buchheit, and B Witten. Industrial Internet of Things Volume G4: Security Framework. Technical report, Industrial Internet Consortium, 2016. URL https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf.

[15] Paul Theron and Alessandro Lazari. The IACS Cybersecurity Certification Framework (ICCF). Technical report, JRC, 2018. URL https://ec.europa.eu/jrc/en/publication/iacs-cybersecurity-certification-framework-iccf-lessons-2017-study-state-art.

[16] Resilient Architectures Workgroup. Resilient Architectures in Railway Signalling. Technical report, AG CYSIS, 2016. URL https://www.seceng.informatik.tu-darmstadt.de/cysis.

# A Connecting Use Cases and Requirements

To show the relation between the use cases and the presented requirements, Table 1 shows which requirement applies to which asset of each use case. The table shows that it is necessary to closely examine cybersecurity on each component of a whole IoRT system, because every asset is assigned several requirements. Vice versa, it shows that all requirements are important as they are valid for multiple of the assets.

| | **Requirement** | **Use Case 1**<br>**Axle Counter** | **Use Case 2**<br>**FOS** | **Use Case 3**<br>**Rolling Stock Monitor** | **Use Case 4**<br>**Level Crossing** |
|---|---|---|---|---|---|
| Provisioning | Hardware Security | Edge Device<br>Temperature Sensor<br>Cloud Server | Light Sensor<br>Processing Unit<br>Storage<br>4G Modem<br>Cloud Server | Sensors<br>LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Electric Sensor<br>Radio Interface<br>Cloud Server |
| | Resources for Security | Edge Device | Processing Unit | (Sensors)<br>Edge Gateway | Radio Interface |
| | Reserve Resources for Updates | Edge Device | Processing Unit | Edge Gateway | Radio Interface |
| | Manufacturer Provides Updates and Support | Edge Device<br>Temperature Sensor<br>Cloud Server | Light Sensor<br>Processing Unit<br>4G Modem<br>Cloud Server | Sensors<br>LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Electric Sensor<br>Radio Interface<br>Cloud Server |
| | Product Security Certification | Edge Device<br>Cloud Server | Processing Unit<br>4G Modem<br>Cloud Server | LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Radio Interface<br>Cloud Server |
| Deployment | Remove or Change Default Credentials | Edge Device | Processing Unit<br>4G Modem | LoRa Interface<br>Edge Gateway<br>3/4G Modem | Electric Sensor<br>Radio Interface |
| | Unique Credentials per Device | Edge Device | Processing Unit<br>4G Modem | LoRa Interface<br>Edge Gateway<br>3/4G Modem | Radio Interface |
| | Remove or Block Unnecessary Physical Interfaces | Edge Device | Processing Unit<br>4G Modem | Sensors<br>LoRa Interface<br>Edge Gateway<br>3/4G Modem | Radio Interface |
| | Disable Unnecessary Services | Edge Device<br>Cloud Server | Processing Unit<br>Storage<br>4G Modem<br>Cloud Server | Sensors<br>LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Radio Interface<br>Cloud Server |
| | Secure Interfaces, APIs and Services | Edge Device<br>Cloud Server | Processing Unit<br>Storage<br>4G Modem<br>Cloud Server | Sensors<br>LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Radio Interface<br>Cloud Server |
| Operation | Logging | Edge Device | Processing Unit | Sensors<br>Edge Gateway | Radio Interface |
| | Strong Mutual Authentication | Edge Device<br>Cloud Server | Processing Unit<br>(4G Modem)<br>Cloud Server | LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Radio Interface<br>Cloud Server |
| | Secure Storage for Credentials | Edge Device | Processing Unit<br>4G Modem | LoRa Interface<br>Edge Gateway<br>3/4G Modem | Radio Interface |

| | Requirement | Use Case 1<br>Axle Counter | Use Case 2<br>FOS | Use Case 3<br>Rolling Stock Monitor | Use Case 4<br>Level Crossing |
|---|---|---|---|---|---|
| | Secure Storage for Data | (Edge Device)<br>Cloud Server | Processing Unit<br>Storage | (Edge Gatway)<br>Cloud Server | Cloud Server |
| | Authorization | Edge Device<br>Cloud Server | Processing Unit<br>Cloud Server | Sensors<br>Edge Gateway<br>Cloud Server | Radio Interface<br>Cloud Server |
| | Accountability and Non-Repudiation | Edge Device<br>Cloud Server | Processing Unit<br>Cloud Server | Sensors<br>Edge Gateway<br>Cloud Server | Radio Interface<br>Cloud Server |
| | Safety and Reliability | Edge Device | Edge Device | Sensors<br>Edge Gateway | Electric Sensor<br>Radio Interface |
| | Input Validation and Data Authentication | Cloud Server | Edge Device<br>Cloud Server | Edge Gateway<br>Cloud Server | Cloud Server |
| | DoS Protection | Cloud Server | Processing Unit<br>4G Modem<br>Cloud Server | LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Radio Interface<br>Cloud Server |
| | Malware Protection | Edge Device<br>Cloud Server | Processing Unit<br>Cloud Server | (Sensors)<br>Edge Gateway<br>Cloud Server | (Electric Sensor)<br>Radio Interface<br>Cloud Server |
| | Identity Revocation and Exclusion of Devices | Edge Device | Edge Device | (Sensors)<br>Edge Gateway | Radio Interface |
| | Backup | Edge Device<br>(Cloud Server) | Processing Unit<br>Storage<br>(Cloud Server) | LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>(Cloud Server) | (Cloud Server) |
| | Secure Communication | Temperature Sensor<br>Edge Device<br>Cloud Server | Light Sensor<br>Processing Unit<br>Storage<br>4G Modem<br>Cloud Server | Sensors<br>LoRa Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Electric Sensor<br>Radio Interface<br>Cloud Server |
| | Security Testing | Edge Device<br>Cloud Server | Edge Device<br>Cloud Server | Edge Gateway<br>Cloud Server | Radio Interface<br>Cloud Server |
| Update | Asset and Configuration Management | All Devices | All Devices | All Devices | All Devices |
| | Monitor Asset Vulnerabilities | Edge Device<br>Cloud Server | Processing Unit<br>4G Modem<br>Cloud Server | LoRA Interface<br>Edge Gateway<br>3/4G Modem<br>Cloud Server | Radio Interface<br>Cloud Server |
| | Secure Update | Edge Device | Edge Device | Sensors<br>LoRa Interface<br>Edge Gateway<br>3/4G Modem | Radio Interface |
| Decommission | Sanitize Device | Edge Device | Edge Device | LoRa Interface<br>Edge Gateway<br>3/4G Modem | Radio Interface |
| | Remove Data Traces from other Devices | Edge Device | Edge Device | LoRa Interface<br>Edge Gateway<br>3/4G Modem | Radio Interface |

**Table 1:** Mapping Use Case Assets to Requirements

# B Overview of References

Table 2 gives an overview of the referenced documents for each listed requirement.

| | Requirement | BITAG IoT Security and Privacy Recomm. [1] | ETSI TS 103 645 [2] | ENISA Good Practices for Security of IoT [3] | ENISA Good Practices for IoT Tool [4] | BSI Cryptographic Mechanisms [5] | BSI IT Baseline Protection: SYS 4.4 [6] | BSI ICS Security Top 10 [7] | GSMA CLP.13 [8] | OWASP IoT Top 10 [9] | NIST Guidelines for Media Sanitization [10] | NIST Digital Identity Guidelines [11] | NIST Framework [12] | Oesterreichs Energie [13] | IIC IIoT G4: Security Framework [14] | IACS Cybersecurity Certification Framework [15] | Resilient Architectures in Railway Signalling [16] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Provisioning | Hardware Security | | ● | ● | ● | | | | ● | ● | | | | ● | ● | | |
| | Resources for Security | | | | ● | | | | | | | | | | | | ● |
| | Reserve Resources for Updates | | | | | | | | | | | | | ● | | | ● |
| | Manufacturer Provides Updates and Support | ● | | | | | | ● | | ● | | | | | | | |
| | Product Security Certification | | | | | | | | | | | | | | | ● | |
| Deployment | Remove or Change Default Credentials | | ● | | ● | | | ● | ● | ● | | | | | | | |
| | Unique Credentials per Device | | ● | | ● | | | | ● | | | | | | | | |
| | Remove or Block Unnecessary Physical Interfaces | | ● | | ● | | | ● | | | | | | | ● | | |
| | Disable Unnecessary Services | | ● | | ● | | ● | | | ● | | | | ● | | | |
| | Secure Interfaces, APIs and Services | | | | ● | | | | | ● | | | | ● | | | |
| Operation | Logging | | | | ● | | ● | ● | ● | | | | | ● | | | |
| | Strong Mutual Authentication | | | | ● | ● | ● | ● | ● | ● | | ● | | | ● | | |
| | Secure Storage for Credentials | | ● | | ● | ● | | | | ● | | ● | | | | | |
| | Secure Storage for Data | ● | ● | | | | | | | ● | | | | | | | |
| | Authorization | ● | | | ● | | | | | ● | | | | ● | | | |
| | Accountability and Non-Repudiation | | | | | ● | | | | | | | | | | | |
| | Safety and Reliability | ● | | | ● | | | | | | | | | | | | |
| | Input Validation and Data Authentication | | ● | | ● | | | | | ● | | | | ● | | | |
| | DoS Protection | | ● | | ● | | | ● | | | | | | | | | |
| | Malware Protection | ● | | ● | | | | ● | | | | | | | | | |
| | Identity Revocation and Exclusion of Devices | | | | | | | | ● | | | | | | | | |
| | Backup | | | | | | | ● | ● | | | | ● | | | | ● |
| | Secure Communication | | ● | | ● | | ● | ● | | ● | | | | | | | |
| | Security Testing | ● | | ● | | | | | ● | | | | | | | | |
| Update | Asset and Configuration Management | | | | ● | | | | | ● | | | ● | | | | |
| | Monitor Asset Vulnerabilities | | ● | | | | | | | ● | | | | | | | |
| | Secure Update | ● | ● | | ● | | ● | | ● | ● | | | | ● | | | |
| Dec. | Sanitize Device | ● | ● | | | | ● | | | ● | ● | | | | | | |
| | Remove Data Traces from other Devices | | | | | | | | | | | | | | | | |

**Table 2:** Overview of References for the Requirements

# A cooperation between

Société nationale des chemins de fer français
Deutsche Bahn AG
Technische Universität Darmstadt
Télékom Paris

*June 2020*