The Internet of Railway Things Security

Whitepaper

Full version

June 2020

SNCF

DB

TECHNISCHE UNIVERSITÄT DARMSTADT

TELECOM Paris

IP PARIS

Contents

Executive Summary

English

Today, the Internet of Things (IoT) is considered together with artificial intelligence (AI) as one of the fastest growing digital technologies in terms of both technical innovations and end-user applications. The Internet of Things is deployed in a vast array of human activities, whether they are industrial (we will speak of Industrial Internet of Things (IIoT)), commercial, military, or civil. There is a natural continuum from IoT to IIoT, to Internet of Railway Things (IoRT), a term that we introduce in this document to account for the particularities due to the rail industry, especially security. The benefits expected from deploying IoT to the railway industry are extremely important from a technological innovation point of view as well as from a business point of view. Lightweight inter-connected computing devices are increasingly utilized in railway transportation to monitor and manage its large and distributed infrastructure required to offer the proper transportation service. With regard to cybersecurity, IoRT has to manage a large attack surface due to physical accessibility to devices as well as other specifics identified in the railway system. Cybersecurity is a topic that has experienced only a relatively limited coverage in the area of IoT given the frequent media reports about disclosed vulnerabilities and security incidents. Needless to say that the IoRT as well requires to be illuminated from a cybersecurity perspective.

To familiarize with the topic, we summarize existing literature discussing the IoT and cybersecurity, which includes the well-known Cisco IoT reference model, and the "Good Practices for Security of IoT" published by the European Union Agency for Cybersecurity (ENISA). We proceed to analyse state-of-the-art radio communication technologies and protocols relevant to the IIoT.

We study the security specifics of IoRT with the help of four use cases selected within railway operations of Deutsche Bahn (DB) and Société nationale des chemins de fer français (SNCF). The use cases cover monitoring rolling stock, level-crossings, track-side rolling stock monitoring (hot box detectors), and track-side monitoring with fiber optic sensing (FOS).

Studying the use cases, we derive and discuss security requirements to protect an IoRT system. The requirements are presented along the lifecycle of an IoRT system with five phases: provisioning, deployment, operation, update, and decommission. Security recommendations for IoRT devices and communication networks represent the foundational defence measures to protect a railway IoT system against cyberattacks. They are intended to be used as guidance for technicians as well as management to come to meaningful decisions.

By synthesizing the common traits of our four use cases and applying the security requirements of the operation phase, we are developing a reference architecture that can be used as a guideline for the design of new IoRT systems. It is not intended to go into technical details, but to provide the reader with key starting points in terms of security and data transmission. All these use cases are deployed along a large network of railway tracks or within numerous rolling stocks. All of them are collecting data in order to be processed in a data center, particularly for predictive maintenance purposes. Accordingly, the reference architecture 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. Several solutions are outlined considering wired or wireless communications. In the case of wired communication, a solution using OPC UA is sketched; in the case of wireless communications, a solution with 5G and slicing is described.

Responsibilities put on IoRT security are manyfold and critical, among them data protection, asset and identity management of devices as well as their physical protection. Our vision for the future comprises further benefits and innovations IoRT can bring to railway operation and again, highlight the critical necessity to design the proper security upfront. It is our belief that IoRT will have to be in operation and already deliver value to the railway industry before considering future innovations such as the connected train or multimodal transportation.

German

Das Internet der Dinge (IoT) wird heute zusammen mit der künstlichen Intelligenz (KI) als eine der am schnellsten wachsenden digitalen Technologien in Bezug auf technische Innovationen und Endbenutzer-Anwendungen betrachtet. Das Internet der Dinge wird in einer Vielzahl menschlicher Aktivitäten eingesetzt, unabhängig davon, ob sie industriell (Industrielles Internet der Dinge (IIoT)), kommerziell, militärisch oder zivil sind. Vom IoT leiten wir über das IIoT bis zum Internet der Eisenbahn Dinge (IoRT), ein Begriff, den wir in diesem Dokument einführen, um die Besonderheiten für die Bahnindustrie zu berücksichtigen, insbesondere für die IT-Sicherheit. Die Vorteile, die durch IoT für die Eisenbahnindustrie erwartet werden, existieren sowohl aus Sicht der technologischen Innovation als auch aus geschäftlicher Sicht.
Leichtgewichtige, vernetzte Geräte werden zunehmend im Schienenverkehr zur Überwachung und Verwaltung der großen und verteilten Infrastruktur, die für die ordnungsgemäße Bereitstellung der Transportleistung erforderlich ist, eingesetzt. In Bezug auf die IT-Sicherheit muss IoRT eine große physische Angriffsfläche verteidigen, außerdem ist die einfache Zugänglichkeit zu Geräten eine Besonderheit im Eisenbahnsystem. Cybersicherheit ist ein Thema, das im Bereich des Internet der Dinge angesichts der Häufigkeit von Medienberichten über offenbarte Sicherheitslücken bisher nur unzureichend behandelt wurde. Daher ist es naheliegend, dass das IoRT auch aus Sicht der Cybersicherheit beleuchtet werden muss.
Um in das Thema einzuführen, fassen wir die vorhandene Literatur zum IoT und zur Cybersicherheit zusammen. Dazu gehören das bekannte Cisco IoT-Referenzmodell und die „Good Practices for Security of IoT“, veröffentlicht von der ENISA. Wir fahren mit der Analyse moderner Funkkommunikationstechnologien und -protokolle fort, die für das IIoT relevant sind.
Wir untersuchen die Besonderheiten der IT-Sicherheit von IoRT anhand von vier Anwendungsfällen, die innerhalb des Eisenbahnbetriebs von DB und SNCF ausgewählt wurden. Die Anwendungsfälle umfassen die Überwachung von Fahrzeugen, Bahnübergängen und die streckenseitigen Heißläuferortungsanlagen sowie Infrastrukturüberwachung mit Fiber Optic Sensing (FOS).
Anhand der Anwendungsfälle leiten wir Sicherheitsanforderungen zum Schutz eines IoRT-Systems ab und diskutieren diese. Die Anforderungen werden entlang des Lebenszyklus eines IoRT-Systems in fünf Phasen dargestellt: Bereitstellung, Inbetriebnahme, Betrieb, Aktualisierung und Außerbetriebnahme. Sicherheitsempfehlungen für IoRT-Geräte und Kommunikationsnetze stellen die grundlegenden Verteidigungsmaßnahmen zum Schutz eines IoRT gegen Cyber-Angriffe dar. Sie sollen sowohl als Anleitung für Techniker als auch als Leitfaden für das Management dienen, um zu sinnvollen Entscheidungen zu kommen. Durch die Synthese der Merkmale unserer Anwendungsfälle und die Anwendung der Sicherheitsanforderungen im Betrieb entwickeln wir eine Referenzarchitektur, die als Richtlinie für den Entwurf neuer IoRT-Systeme verwendet werden kann. Es wird nicht auf technische Details eingegangen, stattdessen werden den Lesern wichtigen Anhaltspunkte in Bezug auf IT-Sicherheit und Datenübertragung gegeben. Die Anwendungsfälle sammeln Daten, um in einem Rechenzentrum verarbeitet zu werden, insbesondere zur vorbeugenden Instandhaltung. Dementsprechend konzentriert sich die Referenzarchitektur hauptsächlich auf den Messdatenfluss von den Sensoren zum IoRT-Rechenzentrum, wo die Daten weiter verarbeitet werden können und Wert für die Eisenbahngesellschaft schaffen. Es werden verschiedene Lösungen für drahtgebunde oder drahtlose Kommunikation beschrieben. Bei der drahtgebundenen Kommunikation wird eine Lösung mit OPC UA skizziert, während bei der drahtlosen Kommunikation eine Lösung mit 5G und Slicing skizziert wird.
Die Verantwortlichkeiten für die IoRT-Sicherheit sind vielfältig und kritisch, darunter der Datenschutz, Asset- und Identitätsmanagement von Geräten sowie deren physischer Schutz. Unsere Zukunftsvision umfasst weitere Vorteile und Innovationen, die IoRT für den Eisenbahnbetrieb bringen kann und unterstreicht die Notwendigkeit, entsprechende Sicherheit im Voraus zu entwerfen. Wir glauben, dass IoRT bereits wertstiftend in den Betrieb eingeführt sein muss, bevor zukünftige Innovationen, wie der vernetzte Zug oder der multimodale Verkehr, angegangen werden können.

French

Aujourd'hui, l'Internet des objets (IoT) est considéré, avec l'intelligence artificielle (IA), comme l'une des technologies numériques dont la croissance est la plus rapide, tant en termes d'innovations technologiques que d'applications pour l'usager. L'IoT se déploie dans toutes les activités qu'elles soient industrielles (on parlera d'Internet *industriel* des objets (IIoT)), qu'elles soient commerciales, militaires ou civiles. La filiation est naturelle de l'IoT à l'IIoT, à l'IoRT, un terme que nous introduisons ici pour tenir compte des spécificités de l'industrie ferroviaire, notamment en termes de sécurité. Les avantages attendus du déploiement de l'IoT sont extrêmement importants tant du point de vue de fonctionnalités nouvelles que du point de vue économique.
Capteurs et composants électroniques intelligents de toute sorte sont interconnectés et sont de plus en plus utilisés pour surveiller et gérer la vaste infrastructure distribuée nécessaire pour répondre aux besoins inhérents au transport ferroviaire. En ce qui concerne la sécurité, IoRT doit gérer une grande surface d'attaque en raison de l'accessibilité physique aux dispositifs par le public ainsi que d'autres spécificités identifiées dans propres aux systèmes ferroviaires.
La cybersécurité n'a fait l'objet que d'une attention relativement limitée dans le domaine de l'IoT sans rapport avec les fréquents articles des médias sur les vulnérabilités et les incidents de sécurité. Il va de soi que l'IoT ne peut se concevoir sans cybersécurité.
Pour se familiariser avec le sujet, nous présentons un bref état de l'art sur l'IoT et de la cybersécurité. Le modèle de référence bien connu de Cisco IoT, ou bien la publication de l'ENISA « Good Practices for Security of IoT » y sont cités. Nous procédons ensuite à une courte analyse des technologies et des protocoles de communication radio les plus récemment déployés dans l' IIoT.
Nous étudions les spécificités de sécurité de IoRT à l'aide de quatre cas d'usage sélectionnés par DB et SNCF dans le cadre de l'exploitation ferroviaire. Les cas d'usage couvrent la surveillance du matériel roulant, les passages à niveau, la surveillance du matériel roulant au bord de la voie (détecteurs de boîtes chaudes) et la surveillance au bord de la voie avec FOS.
L'étude des cas d'usage nous a permis d'établir un nombre d'exigences de sécurité pour protéger un système IoRT. Elles sont présentées tout au long du cycle de vie en cinq phases d'un système IoRT : approvisionnement, déploiement, exploitation, mise à jour et déclassement. Les recommandations de sécurité pour les dispositifs IoRT et les réseaux de communication représentent des mesures de défense fondamentales pour protéger un système ferroviaire IoT contre les cyberattaques. Elles sont destinées à servir de guide décisionnel aux ingénieurs ainsi qu'aux manageurs.
En faisant la synthèse des traits communs de nos quatre cas d'usage et en appliquant les exigences de sécurité de la phase d'exploitation, nous élaborons une architecture de référence qui pourra être utilisée comme ligne directrice pour la conception de nouveaux systèmes IoRT. Elle n'a pas pour but d'entrer dans des détails techniques, mais de fournir au lecteur des éléments clés initiaux en termes de sécurité et de transmission de données. Tous ces cas d'utilisation sont déployés le long d'un vaste réseau de voies ferrées ou au sein de nombreux matériels roulants. Tous collectent des données en vue de leur traitement dans un centre de données, notamment à des fins de maintenance prédictive. En conséquence, l'architecture de référence se concentre principalement sur le flux de données de mesures allant des capteurs vers le centre de données où il peut être traité plus avant et créer de la valeur pour la compagnie ferroviaire. Plusieurs solutions sont présentées prenant en compte des communications câblées (une solution utilisant OPC UA est esquissée) ou sans fil dans ce dernier cas, une solution utilisant la 5G et le « slicing » est rapidement décrite.
Les responsabilités en matière de sécurité sont multiples et critiques, parmi lesquelles la protection des données, la gestion des actifs et de l'identité des dispositifs ainsi que leur protection physique. Notre vision mentionne d'autres avantages que l'IoRT peut apporter à l'exploitation ferroviaire et à nouveau souligne la nécessité de l'accompagner d'une sécurité adéquate. Nous sommes convaincus que l'IoRT devra être en service et dèjà apporter de la valeur au secteur ferroviaire avant d'envisager de futures innovations telles que le train connecté ou le transport multimodal.

1 Introduction

The phrase *Internet of Things* is often attributed to Kevin Ashton (MIT) who coined it in a presentation he gave to Procter & Gamble in 1999. Actually, we can trace several research projects in the early 80-90's that already succeeded to connect and control various objects or things to the Internet. Today, the Internet of Things (IoT) is considered together with artificial intelligence (AI) as one of the fastest growing digital technologies in terms of both technical innovations and end-user applications. Already over 30 billion *smart things* are connected according to many sources and the number is likely to increase in the next several years.

It is worth mentioning that several enabling technologies made this digital revolution possible. Among them, miniaturization and nanotechnology were necessary to reach adequate cost and size; battery technology (and more recently energy harvesting) to offer autonomy and mobility; RFID, wireless and Internet technologies were essential to connectivity and communication; AI for data mining and analytics. Last but certainly not least, cybersecurity and more recently blockchain to bring reliability and trust unleashing a wide range of applications. This unprecedented convergence of technologies is supporting the reunion of operational technology (OT) and information technology (IT) creating a technology continuum from the Micro-Electro-Mechanical Systems (MEMS) or Supervisory Control And Data Acquisition systems (SCADA) – a typical subclass of OT control systems – to machine to machine (M2M) or machine to data center forming today the essence of IoT infrastructure.

There is not one off-the-shelf IoT product today supporting a large community of users. Successful and effective solutions are the result of a consortium of an array of suppliers or device manufacturers developing a fine-grained integration of their respective products under a strong project leadership with crisp specification. The IoT solution must support data that moves from devices to devices overcoming the lack for a unique communication standard. Data is then analysed and processed in data centers or clouds and generates commands and controls to actuators or information to human beings (passengers, train driver, or other employees). This must always be executed in a timely, flexible, and secure manner.

Quick elements of market impact for the railways industry In 2012, GE (General Electric) was predicting a saving of $27 billion in the freight railways industry against 1 % of saving thanks to Industrial Internet of Things (IIoT) usage. More recently, the *TransformingTransport* European H2020 project evaluates that 10 % efficiency improvement may lead to cost savings of 100 billion Euro in freight transportation over Europe [5].

In the same period of time, we could read that the forecast of the growth of the "smart railways" is approaching 15 % for the 5 coming years[1].
The growth is mostly due to the growth of inter-city traffic but also to the integration with an increasing number of sensors and actuators fostering a faster decision making which in turn is supporting an optimized usage of material as well as new business opportunities.
This growth rate is confirmed by other marketing firms like Markets and Markets who sees the smart railways market size growing from about $20 billion in 2019 to $39 billion by 2024, at a compound annual growth rate (CAGR) of 13.7 % during the period[2]. Europe is estimated to hold the largest market size in the smart railways market in 2019 led by countries such as the UK, France, and Germany.

These numbers from various sources are somewhat consistent in terms of order of magnitude. They are all hinting that there truly exists an unmissable business opportunity for the rail industry by optimizing passenger and freight ridership and reducing costs. This is precisely the purpose of IoT.

[1] `https://www.mordorintelligence.com/industry-reports/smart-railways-market`
[2] `https://www.marketsandmarkets.com/PressReleases/smart-railways.asp`

IoT benefits to the rail industry Beyond the mere economic aspects supporting the adoption of IoT technology by the rail industry, it is important to list innovative functionalities or capabilities that IoT brings to the table and would not be possible without, such as:

- An improved and pervasive connectivity is able to support sturdy Internet-based applications and services covering with accuracy the entire passenger travel. More than ever before, passenger experience will be augmented with on-board information or even online entertainment.
- The continuous monitoring and surveillance of material (vs. human random and spot sampling) allows early detection of events like failures or cyberattacks, decreasing safety risks. As a direct consequence, repairs can be done in a timely manner and disaster recovery can be undertaken more rapidly. Predictive maintenance can be efficiently put in place thanks to an increased amount of data.
- High precision, continuous, and real time traffic control and assessments enables an effective asset deployment and optimisation of utilization of the railway's rolling stock.
- In combination with edge computing, IoT supports developing more accurate and timely remote command and control systems. By providing train drivers and other staff with constant communication, IoT allows avoiding to put human beings in dire or dangerous situations.
- An order of magnitude of more data is made available to efficient AI-based algorithms and analytics. An accelerated and better decision making is then possible. Refined analytics, detection of drawbacks and opportunities are allowing envisioning new and more effective business processes or future products.

As we can see, absolutely all artefacts and all stakeholders of the railway industry are potentially impacted by the deployment of the IoT technology making it unavoidable. At last, in a close future, IoT will play an important part in a double transformation of the transportation industry: enabling truly integrated multi-modal travels as well as bearing the promise of a fully automated train: safer, cheaper, more predictable, with an improved quality of experience for the passengers.

1.1 Concepts of IoT

Publications and large international conferences on the IoT are countless. There is even an IEEE Journal dedicated to the topic created in 2014. It is no surprise that many definitions of the IoT have appeared in the past decades depending on the preferred angle to look at it, and it is no surprise that IoT currently has no universally-accepted and actionable definition.
However, standard bodies tend to provide definitions staying as abstract and agnostic as possible. For instance: the following definition of IoT by the IEEE [8] or by the National Institute of Standards and Technology (NIST) [9] does not even mention the word Internet:

> Internet of Things (IoT): a wired or wireless network of uniquely identifiable connected devices which are able to process data and communicate with each other with or without human involvement.

ITU in its recommendation ITU-T Y.2060 also gives an abstract definition but is adding two notes to include services or applications and societal impact:

> A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.
>
> NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.
>
> NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

At last, Cisco is proposing a definition which is this time mentioning the words Internet and things:

> The IoT is a general purpose system of "smart things" (ubiquitous sensors and actuators) connected via the Internet. The Internet of things brings together people, process, data, and machines or "things" turning information into physical actions, and the other way around; creating new capabilities for individuals, businesses (commerce and industry), and eventually entire geographical regions.

Many other definitions can be found in the industry or the academic world. Without attempting to add yet another definition, it is worth mentioning that today, IoT is almost always associated with the notion of big data since it is continuously producing and transmitting data. Then, it is more and more often associated with AI which transforms all the produced data into knowledge. The notion of industrial IoT was then introduced. It must be combined with the global digitization of the industry sometimes called "Industry 4.0".

1.2 From IoT to Industrial IoT (IIoT)

From the IoT, we move on to the definition of Industrial Internet of Things (IIoT), for which the scientific and technical difference is blurry. Only the purpose of this kind of IoT can lead us to determine some difference.
IIoT often refers to the network of machines, sensors, and actuators that run industrial applications. It is considered that OT is at the starting point of IIoT.
The Industrial Internet Consortium (IIC)[3] was founded in 2014 by GE, Intel, IBM, Cisco, and AT&T to bring over 200 industrial partners together to promote Industrial Internet and propose a reference architecture [23].
The IIoT is characterized by the weight of OT versus IT, a longer lifecycle of its devices and its utilization in industrial and manufacturing environments inside plants or warehouses. When utilized for manufacturing, sensors and actuators have to comply to a number of requirements especially in terms of reliability, sturdiness, or controlled Quality of Service (QoS) including accuracy. A control and command center will receive and process data generated by sensors and return commands to cyber-physical systems such as robots or cobots. The presence of actuators may involve critical and stringent real time constraints. In this case some computation will be processed "on the edge" of the sensors and actuators. In other words, sending data all the way towards a remote data center will be avoided and data will be processed as soon as enough computational power is found on the shortest possible path from the sensors to the actuators in order to decrease latency and save energy.
See for instance, for more details: `https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-Internet-things`.

1.3 From Industrial IoT to Internet of Railway Things (IoRT)

After describing IoT and IIoT, we introduce in this document what we understand as Internet of Railway Things (IoRT) to account for the particularities due to the rail industry.
The Internet of Railway Things is a particular IIoT characterized at the very least by its very large size, its topology, its critical need for safety and security. Very few large networks of things are comparable: telecommunication networks or electrical smartgrids do not transport human passengers; planes, ships, or trucks transport passengers and freight but have not this level of near predictability that trains do have. They do not reach the heart of our cities. It must be noticed that planes cannot stop when they receive an alert during a flight, this is a major difference in terms of countermeasures to be taken in case of a cyberattack. The IIoT can and must progressively evolve without stopping the business which imposes new technology and devices to be able to

[3] `https://www.iiconsortium.org`

inter-operate with legacy systems which often generates a vastly heterogeneous network of things. However, one of the main difference to consider in IoRT is its relation to safety-critical systems and the freedom of interference with their safety functions. This explains on of the important aspects of this document. Among the main differences, it is worth mentioning:

- safety criticality: there can be a dozen or more OT assets that, if compromised by a cyber-attack, could cause major disruptions to railway services in a cascading effect. This includes the trains themselves, the station operations, and infrastructure. In turn, insufficient security protection of the assets can have an impact on the safety of the transportation system.
- Sensors or devices placed along the railway track are publicly and easily accessible by an attacker and constitute a specific vulnerability not present in other critical infrastructures.
- Moving human beings and freight along a wide network of railroads, sometimes adding one level of complexity and heterogeneity by crossing country boundaries, constitutes a specific responsibility.
- Specific standards of communication protocols – such as GSM-R and soon Future Railway Mobile Communication System (FRMCS) to replace GSM-R – demand specific verification and validation by the railway industry.

1.4 Instances of Threats to Internet of Railway Things (IoRT)

This section highlights the need to deal with security in IoRT by discussing commonly known attacks to industrial control systems (ICSs), IoT systems and SCADA systems. Railway transportation systems both in America and in Europe have already been subject to several significant cyberattacks. For instance, in 2008, a teenager was able to derail four trams in the city of Łódź, Poland by modifying a TV remote control[4]. In 2012, the United State's Transportation Security Administration noted an attack on railway computers disrupting railway signals for two days[5].
Stuxnet is the most prominent and infamous example for a worm targeting a SCADA system. However, it is also well documented and has been deeply investigated by security researchers worldwide. There are two lessons from Stuxnet that we can learn for the IoRT. First, even air-gapped systems can be infected by worms because Stuxnet propagated through USB flash drives. This highlights the importance to consider all physical interfaces of devices. Second, malware is crafted for specific targets to effectively identify and damage a small set of hardware. For whatever imaginable reason, a sufficiently equipped attacker could identify vulnerabilities in deployed IoRT systems and craft a malware to cause area-wide disruptions in railway transportation.
In Germany, there is a reported case of the ransomware WannaCry infecting the passenger information system[6]. San Francisco's public transport MUNI was infected by a ransomware as well[7], forcing the operator to shut down the entrance gates and allow passengers to ride for free. This shows that auxiliary systems including possible IoRT applications are vulnerable to non-targeted attacks if not protected properly. Such ransomware does not attack a specific system but abuses software vulnerabilities to reach as much dispersion as possible.
Other popular examples of malware include Mirai, Carbanak, Conficker and Emotet. Recent development shows that malware is an ever-changing landscape adapting to countermeasures and designing new attacks to overcome them.
With the growth of the IoT and the wide variety of sensors, the number of vulnerabilities will increase and in turn, the number of attacks will rise accordingly. Thus, it is of paramount importance to closely monitor this landscape to be able to swiftly react to it.

[4] https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/

[5] https://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/

[6] https://twitter.com/Avas_Marco/status/863107445559889921

[7] https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

1.5 Aim and Objectives of this Whitepaper

This document describes cybersecurity recommendations to effectively protect 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 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 are not dealing with railway stations, warehouses, or even the complex railway network of switches when approaching a large railway station. 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, 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 Related Work and Additional Reading

To introduce the reader a bit deeper in the environment of IoT, we present related works for further reading and we analyse existing communication solutions and protocols that are utilized in IoT.

2.1 Related Work and Concepts

We present the state of the art by summarizing work and publications of other scientific groups, enterprises, working groups, and associations, focusing on the most relevant regarding the domain at hand. Table 1 summarizes important aspects of the presented references. We start with relevant works that propose and discuss reference architectures for IoT in general and not necessarily related to security. We then turn to publications with a security focus that provide cybersecurity best practices, countermeasures, or recommendations. The related work is presented to give an overview what other designers of IoT architectures already implemented and to learn from them what is of importance in this whitepaper.

	Definition IoT	Threats	Reference Architecture	Security Best Practices	Use Cases
Cisco Internet of Things Reference Model	–	–	✓	–	–
Internet of Things Architecture	–	✓	✓	–	✓
GSM Association	✓	–	✓	✓	✓
NIST SP 800-160 Volume 1 and 2	✓	✓	–	✓	✓
Oesterreichs Energie	–	–	–	✓	✓
BITAG	✓	✓	–	✓	–
BSI: IT Baseline Protection	–	–	–	✓	–
BSI: ICS Security Top 10	–	✓	–	✓	–
ANSSI: Referentiels d'exigences	–	–	–	✓	–
ENISA Good Practices for Security of IoT	–	✓	–	✓	✓
ENISA Good Practices for IoT Tool	–	✓	–	✓	–
ETSI TS 103 645	–	–	–	✓	–
OWASP IoT Top 10	–	✓	–	–	–

Table 1 – Overview of related works

Cisco Internet of Things Reference Model Cisco has published a white paper titled "The Internet of Things Reference Model" containing a reference model structuring the IoT into seven functional layers [19]. The reference model is depicted in Fig. 1. Each layer is described in detail focusing on data flow and device types used. In particular, it introduces the notion of edge computing (which is critical to address low latency requirements and to deal with alerts) and integrates OT with IT providing us with a global vision going from the small sensors to users collaborating through business processes via a cloud which plays a central role of accumulating data for the benefit of applications. The reference model is well-suited to structure an IoT architecture. However, the only claim regarding security is that measures must be pervasive on all levels of the reference model. In a way, it is seen as a unique cross layer activity. For instance, Intel this time is looking at security in cooperation with McAfee[8].

[8] `https://www.intel.fr/content/www/fr/fr/internet-of-things/white-papers/developing-solutions-for-iot.html`

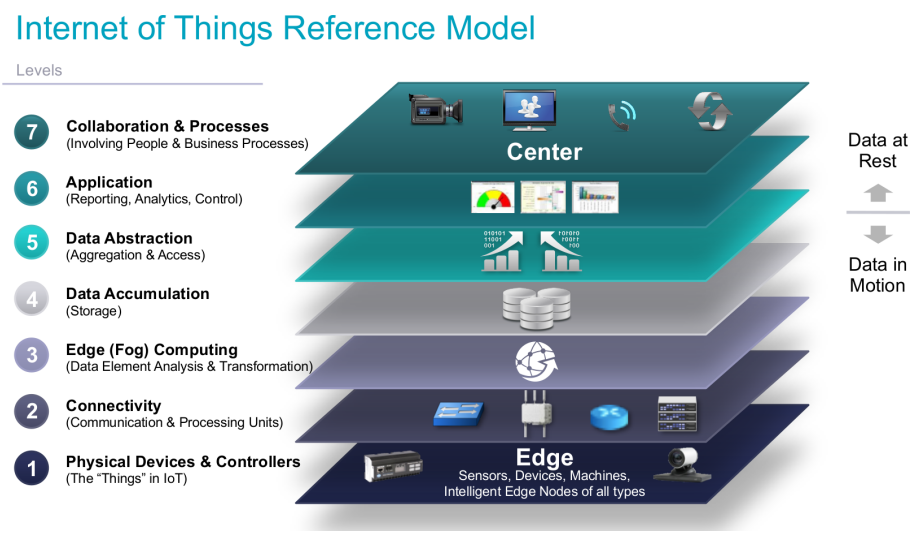

Figure 1 – CISCO IoT Reference Model [19]

Internet of Things Architecture The IoT-A project has developed an architectural reference model for the IoT and published it in [4]. The reference model consists of five sub-models: a domain model, an information model, a functional model, a communication model, and a trust, security & privacy model as shown in Fig. 2. The domain and information sub-models are specified with the Unified Modeling Language (UML). They can be used to formally describe and structure an IoT use case. Their security model includes a discussion about security in constrained and unconstrained communication networks, as this is a frequently appearing issue in Io(R)T. The security model also covers application security where system safety is addressed as we often find it in railway applications as well. They mention the fail-safe property that is central to such safety systems, but do not investigate interference of security measures.

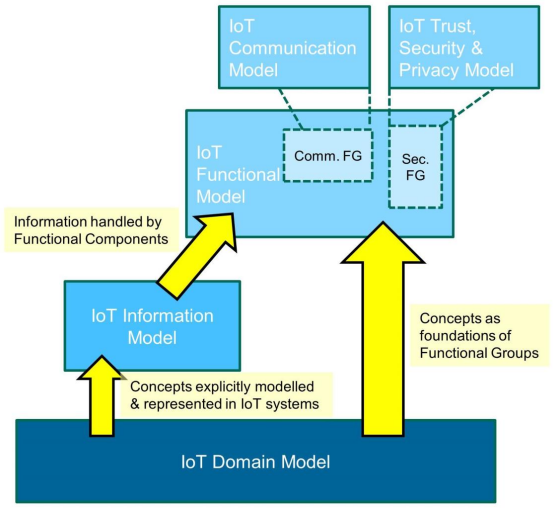

Figure 2 – Overview of the sub-models defined by the reference model of IoT-A [4]

GSM Association The GSM Association (GSMA) is a trade body that represents the interests of mobile network operators worldwide. The association has created a set of security guidelines for the benefit of service providers who are looking to develop new IoT services. The documents address a multitude of audiences, including IoT Service Providers, IoT Device Manufacturers, IoT

Developers, and Network Operators. It consists of five documents, an overview of their relation is given in Fig. 3.

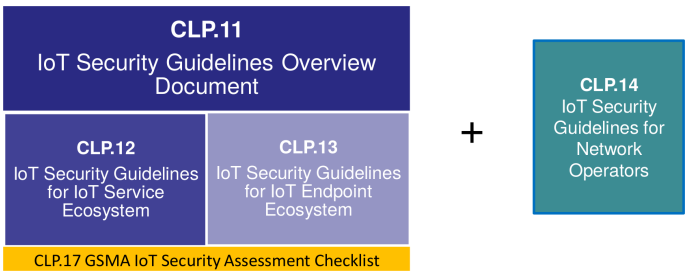

Figure 3 – GSMA IoT Security Guidelines Document Structure [20]

GSMA follows a simpler IoT model than Cisco's IoT Reference Model shown in Fig. 1. But the model is similar in its layout with endpoint ecosystems (edge devices) comprised of comparatively low resources. The endpoints are able to communicate via various types of communication networks to send the gathered data to a service provider who does further data processing. A visualization of the example IoT Model is given in Fig. 4.

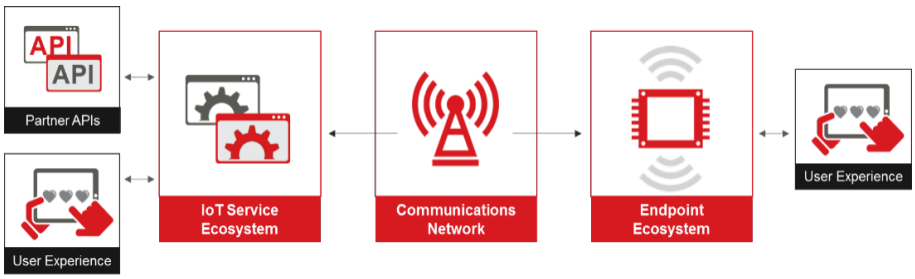

Figure 4 – GSMA Example IoT Model [20]

The set of security guidelines provides detailed recommendations on the security of endpoints, networks and services. This underlines if this was necessary, the importance of focusing on security in this whitepaper. They are concentrated in a security assessment checklist that allows demonstrating the security measures an organisation has to take in order to protect its products, services, and components from cybersecurity risks.

NIST SP800-160 Volume 1 and Volume 2 The NIST has published a technical report detailing cybersecurity and resilience for systems as Special Publication 800-160. Volume 1 is titled *Systems Security Engineering* [28] and Volume 2 *Developing Cyber Resilient Systems: A Systems Security Engineering Approach* [30]. The Special Publication is not explicitly targeted on IoT but claims its applicability to the domain and provides a definition of IoT as well. It is sometimes mentioned by IoT experts as a reference document for cybersecurity and thus as well relevant to our whitepaper. Topics discussed in the publication include cyber resiliency goals and objectives, techniques and approaches, design principles, cyber resiliency lifecycle processes as well as practical examples.

Oesterreichs Energie "Oesterreichs Energie" is an association of Austrian electricity companies. They have published a catalogue of requirements for the end-to-end security of smart meters [32]. Their catalogue is applied to the very specific example of a smart meter architecture much more concrete than the use cases described in Section 3. Described are edge and cloud devices, human-machine interfaces as well as users and their roles. Requirements for the devices are categorized into generic, data integrity, backup, access control, confidentiality, audit, and lifecycle groups. Finally,

the authors provide an example of applying their proposed requirements. The practice oriented content and structure of the listed requirements provide a good example how specific requirements for a IoRT device could be designed.

BITAG The Broadband Internet Technical Advisory Group (BITAG) is an organization focused on bringing together engineers and technologists to develop consensus on broadband network management practices and other related technical issues. In 2016, the BITAG published a whitepaper entitled "Internet of Things (IoT) Security and Privacy Recommendations" [7]. The report discusses common IoT security issues such as insecure communication networks, data leaks, malware, service disruption, and updatability. It provides recommendations to mitigate the effects of the discussed security issues focused on home IoT devices and less on IIoT that are of value if applied to IoRT. A variety of known incidents are referenced to justify the given recommendations.

BSI: IT Baseline Protection The IT Baseline Protection published by the German Federal Office for Information Security (BSI) contains a module covering general IoT devices (SYS.4.4) [17] which provides examples for relevant requirements. It features common threats to IoT devices as well as basic requirements to protect them such as authentication, secure updates, access control, utilization of secure transport protocols, asset management as well as decommission of the devices.

BSI: industrial control system Security Top 10 Threats and Countermeasures The German Federal Office for Information Security (BSI) regularly publishes a technical report about the ten most frequent cyber threats on industrial control systems.. The latest issue from 2019 is entitled "Industrial Control System Security Top 10 Threats and Countermeasures 2019" [18]. The list of threats is depicted in Fig. 5, it is compiled from security-specific incidents, threat intelligence reports and reports from the industrial sector that is required to notify the BSI in case of substantial IT incidents. As German information security regulator, publications of the BSI are very relevant to IoRT security.

Top 10 Threats	Trend since 2016
Infiltration of Malware via Removable Media and External Hardware	↗
Malware Infection via Internet and Intranet	↗
Human Error and Sabotage	↑
Compromising of Extranet and Cloud Components	↑
Social Engineering and Phishing	↘
(D)Dos Attacks	↑
Control Components Connected to the Internet	→
Intrusion via Remote Access	→
Technical Malfunctions and Force Majeure	↘
Compromising of Smartphones in the Production Environment	→

Figure 5 – BSI Top 10 Threats to industrial control systems [18]

The report contains a detailed description of each threat as well as recommendations for countermeasures on technical and operational level. It also provides a self-check to assess a company's current state of IT security and identify the areas requiring immediate attention.

ANSSI: Requirements Referential Agence nationale de la sécurité des systèmes d'information (ANSSI) is the French counterpart of the German BSI. Since 2010, these two agencies agreed to work together to strengthen protection measures against cyberattacks. ANSSI regularly updates a list of reports on referential of best in class protection measures [1]. ANSSI has also put in

place evaluation centers where tests of compliance to various security and trust regulations are conducted.

ENISA Good Practices for Security of IoT In "Good Practices for Security of IoT", the European Union Agency for Cybersecurity (ENISA) describes IoT security with a focus on software development guidelines [11]. It is mainly targeted at software developers, integrators and platform and system engineers and with that focuses on software while our whitepaper is aimed more broadly to also include the hardware. The study follows a 6 phase software development life cycle (SDLC) that is reproduced in Fig. 6. The SDLC contains comparable phases to the IoRT lifecycle we later present in Section 4.

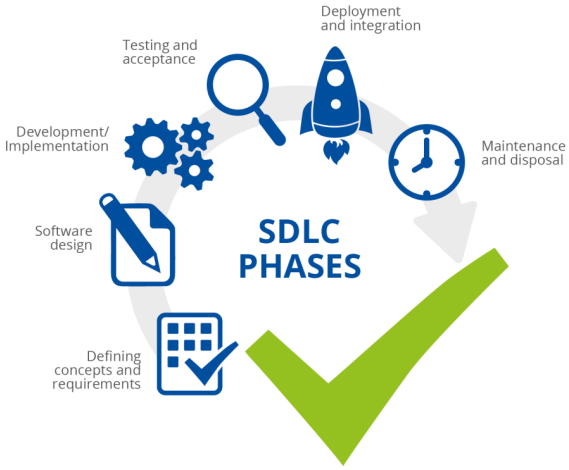

Figure 6 – ENISA software development life cycle [11]

The study refers to STRIDE[9] as a commonly used methodology to identify threats (threat modelling) and presents an exhaustive threat taxonomy which can serve as template in the IoRT context. The taxonomy is very relevant, as ENISA is the European cybersecurity regulator. The study provides an asset taxonomy as well which however is of less importance to the focus of our whitepaper.

ENISA Good Practices for IoT and Smart Infrastructures Tool The European Union Agency for Cybersecurity (ENISA) has published a tool that intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure that have been published the last years [12]. The tool provides an extensive collection of security practices of various thematic areas and security domains. ENISA, as an European agency, is very relevant for critical infrastructures including railway transportation. It cooperates with national cybersecurity agencies like BSI and ANSSI to serve as the basis for certification of products, processes and services that support the delivery of the Digital Single Market. Beyond collecting best practices which are valuable to derive recommendations for IoRT, the tool references several further relevant publications such as standards like ISO 27000 series, NIST SP 800-30, NIST SP 800-53, and publications like BSI IT Baseline Protection, OWASP, GSMA, and more.

ETSI TS 130 645 ETSI's technical specification TS 103 645 *Cyber Security for Consumer Internet of Things* aims at the IoT for consumers [10]. The publication contains guidelines for cybersecurity that coincide with the recommendations we found in other publications.

[9] **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service and **E**levation of Privilege

OWASP IoT Top 10 The well-known OWASP Foundation[10] has launched a project to gather the most important issues of IoT security. The project published the latest top 10 list of issues in 2018 [26]. The list is reproduced in Table 2, while the publication contains a more detailed description of each issue. It is very relevant to IoT practitioners and hence our whitepaper, because the list is compiled from industry feedback.

I1	Weak Guessable, or Hardcoded Passwords
I2	Insecure Network Services
I3	Insecure Ecosystem Interfaces
I4	Lack of Secure Update Mechanism
I5	Use of Insecure or Outdated Components
I6	Insufficient Privacy Protection
I7	Insecure Data Transfer and Storage
I8	Lack of Device Management
I9	Insecure Default Settings
I10	Lack of Physical Hardening

Table 2 – OWASP IoT Top 10 Overview

2.1.1 Relevant Standards

Broad application of IoT and in particular the inclusion of security concepts is a comparatively new topic. On the contrary, defining standards is a process that can take several years until a document converges towards the acceptance of a multitude of stakeholders in the standards creation process. This is the reason why no document has emerged yet that can be considered a IoT standard dealing with cybersecurity. This will most likely change in the future while more and more IoT systems are deployed and the cybersecurity awareness increases as more security vulnerabilities become public. Two existing general security standards should be mentioned in the context of this whitepaper. ISO 27001 is a standard that deals with information security management and could as well be applied to the management of IoT and IoRT systems. The IEC 62443 standard series defines security requirements on system and component level depending on the level of protection derived from a conducted security risk analysis. It is actually a standard series targeted at ICSs and OT but often applied to related systems while no specific standards exist, because it is one of the most comprehensive security standards currently available and covers security at a large range of level of detail.

2.2 Analysis of Radio Communication Solutions for IoT

This section presents several long range standard telecommunication technologies widely used in various different IoT application contexts. The existing solutions will be compared according to several criteria:

- Duplexing and multiple Access.
- Frequency bands of operations.
- Physical layer features (modulations, error codes, ...).
- Technology optimization techniques for IoT (Discontinuous reception, monitoring, and sleeping modes).
- QoS provided to applications.
- Load assumptions.

Three families of IoT standard solutions are analysed in the following paragraphs:

[10] `https://owasp.org`

- 3GPP Based solutions: Extended Coverage GSM (EC-GSM), Long-Term Evolution (LTE), Narrowband IoT (NB-IoT), 5G.
- IEEE based solutions: IEEE 802.11ah, IEEE 802.15.4, Bluetooth LE, ZigBee.
- Low Power Wide Area Networks (LPWAN) solutions: Sigfox, Long Range (LoRa).

3GPP Based solutions: EC-GSM, LTE, NB-IoT, 5G. 3GPP Based solutions have been designed to operate in licensed bands. Extended Coverage GSM are 2G technologies. They rely on a Frequency Division Multiple Duplex (FDD) duplexing scheme and use a Time Division Multiple Access (TDMA) multiple access method. EC-GSM relies on 200 kHz channel bandwidths. LTE is a low power wide area network (LPWAN) radio technology. Technical details can be found in [6]. LTE for Machines (LTE-M) has been designed specifically, for machine-to-machine and IoT applications. It reuses classical LTE infrastructure but makes use of a lower bandwidth of 1.4 MHz. It provides also bidirectional communications. It uses 15 kHz subcarriers in downlink and uplink. 16-QAM modulation can be used in downlink and specific power saving modes (PSM) and discontinuous reception algorithms (eDRX) have been designed to reduce energy consumption of sensors. NB-IoT is a FDD system that relies on Orthogonal Frequency Division Multiplex Access (OFDMA) multiple access scheme. As shown in Table 3. It uses 15 kHz subcarriers in downlink. In uplink, two subcarriers sizes have been defined: 15 kHz and 3.75 kHz.

IEEE based solutions: 802.11ah, 802.15.4, Bluetooth LE, ZigBee. IEEE Based solutions have been designed to operate in Industrial Scientific and Medical (ISM) bands. IEEE 802.11ah introduces some technology optimization for IoT applications. It provides a trade-off at physical/MAC layer in terms of power, range, and data rate. The IEEE 802.11ah layer is based on IEEE 802.11ac with data rates higher than 100 kbit/s. Some specific mechanisms have been introduced to provide highly robust links and low power consumption required for battery operated devices. It can be used on sub GHz unlicensed bands. Range can be up to 1 km due to improved propagation characteristics of sub GHz radio waves. Typical applications of IEEE 802.ah are large scale low power sensor networks, smart meter, video surveillance, or wearable consumer electronics. It can also be used as a backhaul for aggregated sensor and meter data. IEEE 802.15.4 is a standard designed to address smart home networking, industrial control, or building automation applications. It can support long battery life and typical data rates are 250 kbit/s, 40 kbit/s, and 20 kbit/s. IEEE 802.15.4 specifies physical and MAC layers for LoWPAN networks. Upper layers are not developed by IEEE 802.15 Working Group. Standards or working groups, such as ZigBee Alliance, implement upper layers to enable multi-vendor interoperable solutions. 6LoWPAN is an IETF Working Group. It defines how IPv6 protocol stack must be implemented on top of IEEE 802.15.4. Physical and MAC layers are based on IEEE 802.15.4. An adaptation layer is added between the MAC and the network layer (IPv6) to provide header compression (IPv6 headers are to large for IEEE 802.15.4), packet fragmentation, and reassembling (to handle size mismatch between IPv6 packets and IEEE 802.15.4 frames).

LPWAN solutions: Sigfox, LoRa Both Sigfox and LoRa solutions have been designed to operate in ISM bands mostly on sub-1 GHz band. Sigfox defines an ultra narrow band communication system. Devices require a Sigfox modem and Sigfox network. Sigfox provides ultra low throughput (100 bit/s). A Sigfox device can send up to 140 messages/day, each message is up to 12 bytes. In uplink, it is possible to send 12 bytes messages up to 140 messages/day. In downlink, 8 bytes messages can be sent up to 4 messages/day Sigfox uses 868 MHz in Europe and 902 MHz band in USA. It relies on frequency hopping (200 kHz). Uplink transmission is based on DBPSK modulation. Downlink transmission relies on DL:GFSK modulation. Sigfox has low power consumption devices that can provide up to 20 years of battery life. It provides also long range communications (up to 40 km in rural area and 3-9 km in urban area). Target applications are smart metering, pet tracking, smoke detection, agriculture, etc. LoRa operates on different ISM bands: 868 MHz and

433 MHz in Europe, 915 MHz in the US and 430 MHz in Asia. It uses a chirp modulation (125 kHz bandwidth) and provides a data rate of 300 kbit/s. LoRa has many applications particularly in IIoT.

Standards	**Frequency Band**	**Range**	**Data Rate**	**Maximum Bandwidth**
LTE-M	LTE band	1000 m	200 kbit/s - 1 Mbit/s	1.4 MHz
NB-IoT	LTE band	1000 m	$<$ 250 kbit/s	180 kHz
IEEE 802.11ah	Sub GHz	1000 m	150 kbit/s - 78 Mbit/s	1 - 16 MHz
IEEE 802.11p	5.8 GHz - 5.9 GHz	1000 m	1.5 - 54 Mbit/s	5/10/20 MHz
Bluetooth LE	ISM $<$ 2.4 GHz	50 m	1 Mbit/s	1 MHz
IEEE 802.15.4	ISM $<$ 2.4 GHz	10 m	40 kbit/s - 250 kbit/s	1 MHz
LoRa	ISM $<$ 863 - 868 MHz 434 MHz	10 km	18 bit/s - 37.5 kbit/s	1 MHz

Table 3 – Comparison between different IoT technologies [37]

2.3 Analysis of Protocols Compliant with Industrial IoT

Open Platform Communication Unified Architecture (OPC UA) is an open source technology defined by 14 specifications booklets from the OPC Foundation (about 1250 pages) available at `http://www.opcfoundation.org`. It is the successor of OLE for Process Control (OPC) which was a proprietary technology. Since 2011, it has been an IEC standard known as IEC 62 541 [13]. OPC UA standard is mainly dedicated to industrial automation allowing data and services interoperability from the sensors and actuators floors to the enterprise cloud.
Its specification describes a middleware for secure data transfer in client-server mode and/or in PubSub mode (i.e. IoT mode), an information model for structuring data, different services for securely accessing and processing data and many other technologies such as redundancy, finite states machine, historical data management, etc. It can use various data transfer protocols such as TCP/IP or HTTPS in client-server mode as well as UDP, Advanced Message Queuing Protocol (AMQP) and Message Queuing Telemetry Transport (MQTT) (Message Queuing Telemetry Transport) in PubSub mode.
Security [15] is a primary concern of OPC UA. It has been fully approved by BSI in Germany [3], ANSSI in France, and by many organizations such as Industrie 4.0, China 2015, MDIS (Oil and Gas Majors) or ICC and NIST in USA. The *OPC UA Part 2* booklet describes how OPC UA protects itself from a listed set of known threats.
OPC UA uses an information model which is object oriented and extensible. It allows to model, with types and instances, the data, the sensors, the actuators and all the machines we are dealing with. This model is put inside what is called the information space or address space which is located inside every server and is normally readable by clients using the OPC UA services. We could use it to model any rolling stock, even a full train.
The OPC UA Foundation encourages industrial organizations to provide standard OPC UA modellings of their artefacts. There are many OPC UA Companion Specifications that provide a way to unify parts of the industry. For instance the *MDIS OPC UA Companion Specification* enables many standards shared by Oil and Gas companies.
OPC UA can be implemented in nearly all operating systems. However, OPC UA defines many functionalities and not all hardware are able to implement everything. That's why OPC UA has split the functionalities into groups and has defined server and client profiles.
The weaker server profile is called a *Nano Embedded Device Server* and can be implemented on hardware with less than 200 kB of memory space (program+data).

Why to use OPC UA for IoRT? The main reasons are summarized below:

- OPC UA is open and its specification continues to evolve and to be enriched.
- OPC UA is standardized allowing easy integration of commercial off-the-shelf (COTS).
- OPC UA is secured. Its security model is recognized by BSI, ANSSI and other organizations.
- OPC UA is portable, scalable and allows many communication technologies and paradigms.
- OPC UA allows the modelling of data and machinery.
- OPC UA can cover the whole process of IoRT as stated below.

It can be noted that SST (Signaling Siershahn GmbH) has been awarded the contract for the implementation of DBMAS (DB Signaling System). SST and DB Netz AG (DB Network), after evaluating further options and a proof-of-concept using a test implementation, made a joint decision to use OPC UA for implementing the client-server communication in DBMAS because OPC UA met all requirements [14].
If we look at the Cisco-IBM-Intel architecture reference model described in Fig. 1, OPC UA could cover the level 3 (Edge Computing) because OPC UA clients were designed for that purpose. It also covers level 4 (Data Accumulation) using Historical Data Access. It covers level 5 (Data Abstraction) through data and machinery modelling. Meanwhile, the lower level 2 (Connectivity) is implemented using OPC UA to transfer data. The upper level 6 (Application) may be built from an OPC UA Client. With HDA (Historical Data Access) services, OPC UA can be used to store data in railways data base, that is level 4. The modelling of OPC UA can be used for level 5 (Data Abstraction). And OPC UA services can be used for edge computing at level 3 (Edge or Fog computing).

Example. Assume that you have sensors monitoring "open-closed" state of the level crossing barriers (see Use Case 4 in Section 3 for a detailed description). These sensors could be managed by OPC UA nano servers. Cloud applications could subscribe to these OPC UA servers as OPC UA clients. Before a train can run, it can automatically subscribe to all the servers in all level crossing barriers on its path and, of course, unsubscribe when it reaches its destination. See Fig. 7.

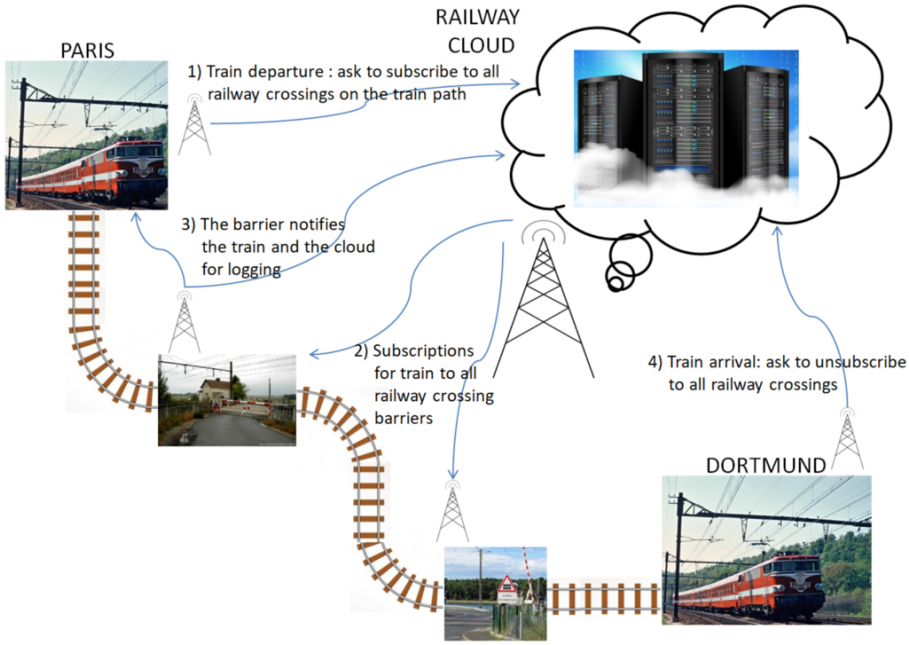

Figure 7 – OPC UA: Paris-Dortmund railway trip

Another way to present the same thing is to use OPC UA - MQTT with brokers as in Fig. 8. There

exist OPC UA servers, acting as publishers, at each level crossing barriers. OPC UA clients, acting as subscribers, are located in the trains and in the cloud. There exist MQTT local brokers on the edge gateways for receiving and dispatching data from the sensors to its subscribers. These brokers may dispatch data to the train and to the cloud, maybe via another broker.

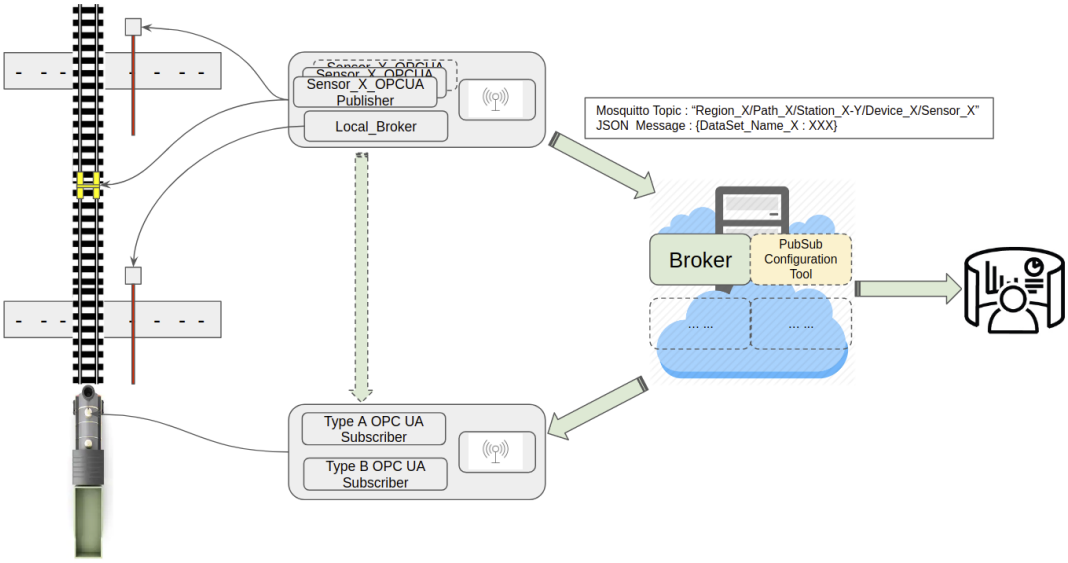

Figure 8 – OPC UA – MQTT: a view with brokers

In Section 5.2, an instantiation of the reference architecture for the case where transmission uses wired communication technology and OPC UA with the client protocol stack at the level of the data center is given (Fig. 23).

3 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.

Use Case	Dimension	Safety	Exposure	Data protection	Communication	Computing	Usage
UC1: Axle counter	Thousands of sensors	SIL4	Accessible to public	Comm protocols	X25 then Ethernet FRMCS	Edge computing Private Cloud	Predictive maintenance
UC2: Fibre optic	<40km	SIL0 Could increase in the future	Accessible to public	Comm protocols	4G/5G SMS towards relevant users	Private Cloud	Predictive maintenance
UC3: Rolling stock	Selection of trains	SIL0	Some tamper resistance	Comm protocols + encryption Detection	LoRa , LTE-M 4G/5G FRMCS	Edge computing Private Cloud	Predictive maintenance
UC4: Level crossing	Selection among 15300 levels in F.	SIL0 & SIL4	Some tamper resistance	Comm protocols + encryption	LTE M 4G/5G FRMCS	Critical RT Edge computing Private Cloud	• Predictive maintenance • Accident detection

Table 4 – Overview of use cases

The use case description in the following sections adheres to the same structure to ease reading and enhance comparability. A summary of all use cases and important properties is given in Table 4. One of the important properties of the use cases is their safety criticality. By definition, the safety criticality is the assigned safety integrity level (SIL) according to EN 50129. The difference between the SILs is the probability with which a system fails. The higher the SIL the lower the probability has to be, with 10^{-9} failures per hour at SIL 4. We consider a use case safety-critical, if the considered IoRT system is or would be assigned a SIL greater than zero (> 0). In our use cases, it is only relevant whether the system is safety-critical or not. The concrete SIL is not from importance. Intuitively, a system is safety-critical if a failure, malfunction or its unavailability could cause financial loss, injuries, or death.
In the context of this whitepaper, it is important to distinguish between safety and security. Safety describes actions and measures to protect humans from failing or malfunctioning systems to avoid injury or death. Security describes actions and measures to protect a system from intentionally maliciously acting humans. Thus, security influences safety, as a system under attack is likely to be unable to meet its safety requirements. Figure 9 visualizes the described relation between safety and security.

3.1 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

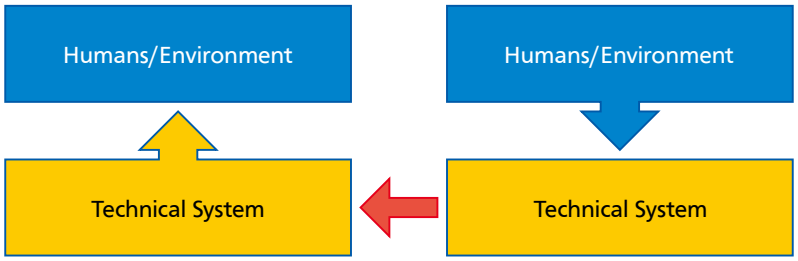

Figure 9 – Schematic relation between safety and security [22]

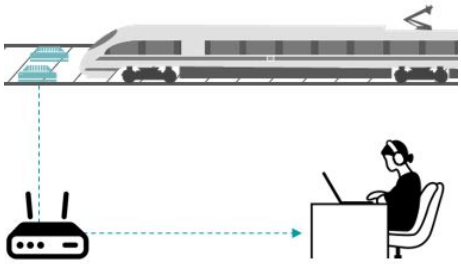

Figure 10 – Axle counter with temperature sensor

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.
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.

3.1.1 Safety Criticality

We distinguish two sensors in this use case: the axle counter and the temperature sensor. The axle counter is safety critical because a fault in the train detection system could provoke the collision of trains if an occupied track section is not correctly detected (false negative). Hence, the axle counter is a SIL 4 system according to EN 50128/50129. The hot box detection, however, is not safety-critical in that sense as it is considered an auxiliary system.

3.1.2 Business Segment

The combined axle counter and hot box detector is operated by a railway infrastructure provider. The collected data about journal bearing temperatures can be used by the infrastructure provider

to avert damage to the infrastructure and the rolling stock using the tracks. It can as well be offered as a service to the rolling stock owner for deriving further information about the condition of its fleet.

3.1.3 Distinction from Conventional IoT

A salient property of this use case is its exposure to the public space. The sensors are located close to the railway tracks that, in many countries, effectively do not utilize access control or surveillance. Thus, benign as well as vicious persons can easily access the tracks physically and the IoT sensors next to it while remaining undiscovered.
Compared to railway IoT, the edge devices of private IoT networks and most industrial IoT networks are accessible by a limited number of persons only. An example is the access control of factory premises.
Railway transportation is classified as critical infrastructure in many countries including the European Union and its member states. Disruption in the railway service could have a significant impact on our society. Therefore great attention should be drawn to the safety and security of train operation and any IoT system deployed there.

3.1.4 Security Impacts

The unavailability, malfunction, or manipulation of the axle counter or the temperature can only lead to critical situations if they coincide with additional circumstances. E.g. a miscount of the axle counter and a division of a train must occur at a same time such that an occupied track section remains undetected, such as a second train might be allowed to enter it.
To run an attack on the temperature measurements, an attacker would need to suppress multiple alerts of hot box detectors in our use case to induce damage or a fire provoked by an overheated bearing. A false positive of any of the sensors (potentially provoked by an attacker) will degrade the capacity of the affected track. Due to the reduced availability, delays will occur and probably loss of reputation for the involved railway companies but no hazardous situation for a train (collision, derailment). Besides, a high amount of false positives presented to a human to take according actions will most likely lead to the alerts being taken less seriously due to familiarization. This can increase the chance for a true positive to slip through the check of an operator without being treated properly.
Widely rolled-out IoT devices harbour the danger of large scale attacks. Reducing the availability of a single track and delaying a few trains might be unfortunate for the involved passengers and customers. Disrupting train service in a significant part of a country would certainly have an impact on the whole society. This underlines the necessity to protect the IoT devices of this use case against cyberattacks.
Physical access to the edge devices is possible. Physical attacks can be used to disrupt the service the edge devices provide, as described above. Additionally, they can be used as an entry point to penetrate devices closer to the system's core or sharing the transmission system.

3.1.5 IoT Model

Data Collection The data is collected via an infrared temperature sensor and a sensor that detects changes in a magnetic field induced by the train axle respectively. An information tuple comprising a timestamp, the axle number, and the temperature value is generated. The sensors are operated by proprietary, embedded hardware. Hardware resources are tailored to the requirements of the application.

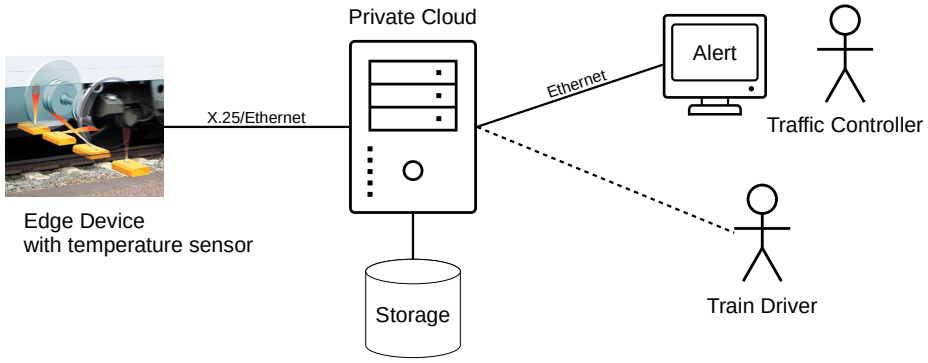

Figure 11 – Axle counter with temperature measurement architecture

Data Transmission In current applications of the use case, data is transmitted via distinct line connections and protocols (e.g. X.25[11]). The data is sent, once an alert is raised, i.e. a train passes the sensor and the bearing temperature is measured to be above a threshold. In future applications, Ethernet transmission via shared connections are possible. Also FRMCS could be utilized in the future. The transmission frequencies for the shared media air in FRMCS are strictly regulated by national authorities. However, this does not prevent an attacker from eavesdropping, jamming, or even transmitting without permission on the frequencies.

Data Structuring Edge computing is performed because currently the hot box detector computes whether an alert is risen by a given measurement or not. This could be shifted more towards the cloud with the combined axle counter/hot box detector scenario, because the data is required by subscribers to infer more information.

Data Processing The temperature data is processed and persisted in a private cloud where decisions are drawn to raise alerts. In order to stop the train, an alert of a hot bearing needs to be forwarded to a railway station the train is soon to pass according to its schedule. Also the train driver can be notified of overheated bearings on his or her train, if means of communication and addressing exist.

3.2 Use Case 2: Fibre Optic Sensing (FOS)

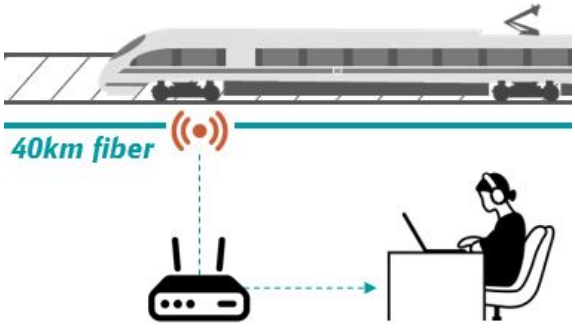

Figure 12 – A 40 km Fiber Optic Sensing capturing the speed of a train

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

[11] https://www.itu.int/rec/T-REC-X.25-199610-I

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.

3.2.1 Safety Criticality

The FOS system and the information it provides are not safety critical. It is assigned SIL 0 according to EN 50128/50129 as it provides supplemental information but does not provide any safety functionality.

3.2.2 Business Segment

The FOS system is operated by a railway infrastructure provider. The collected data can be used by the infrastructure provider to avert damage to the infrastructure and the rolling stock using the tracks caused by the incidents described above. It can as well be offered as a service to the rolling stock owner for deriving further information about the condition of its fleet.

3.2.3 Distinction from Conventional IoT

As in the previous use case, FOS along railway tracks differs from conventional IoT in the public accessibility and the difficulty to employ strong (physical) access control.

3.2.4 Security Impacts

FOS does not provide safety-critical functionality. Thus a failure or attack can only have low impact on train operation. In the worst case, the availability of the train service falls back to the level it had without the deployment of FOS, as it is today. Manipulation of FOS by an attacker could be used to disguise cable theft.
Physical access to the edge devices is possible. Physical attacks can be used to disrupt the service the edge devices provide or to use them as an entry point to penetrate devices closer to the system's core or sharing the transmission system.

3.2.5 IoT Model

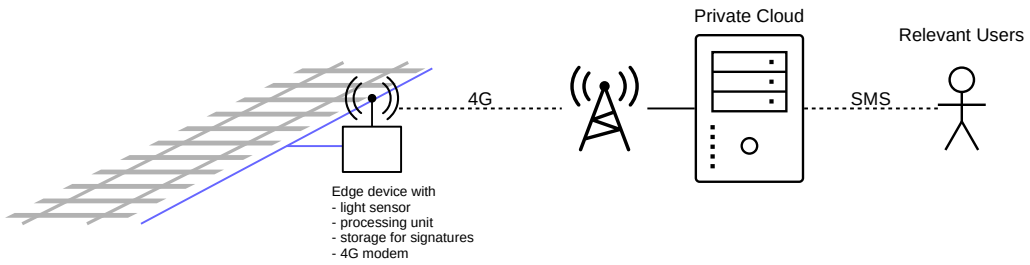

Figure 13 – FOS architecture

Data Collection Proprietary FOS devices are attached to a dedicated fibre optic cable to continuously measure the reflection properties of the cable. The measurements are matched against signatures to provide a data tuple comprising an event type and the localization of the occurred event. The sensors are operated by proprietary, embedded hardware. Hardware resources are tailored to the requirements of the application.

Data Transmission Measurements are sent over the air via a 4G modem. Hence, the transmission media is shared and can be jammed or – without proper protection – eavesdropped by an attacker.

Data Structuring Signatures of measurements are required to be evaluated in the track-side equipment (edge computing). The amount of data generated by FOS is infeasible to be transmitted towards a centralized cloud. It is more efficient to perform the computing on the edge devices.

Data Processing A centralized entity (private cloud) receives the events generated by the edge devices. The centralized entity alerts responsible people (e.g. via SMS) of the event. They can then decide on further actions to react to the raised event.

3.3 Use Case 3: Rolling Stock Remote Monitoring System

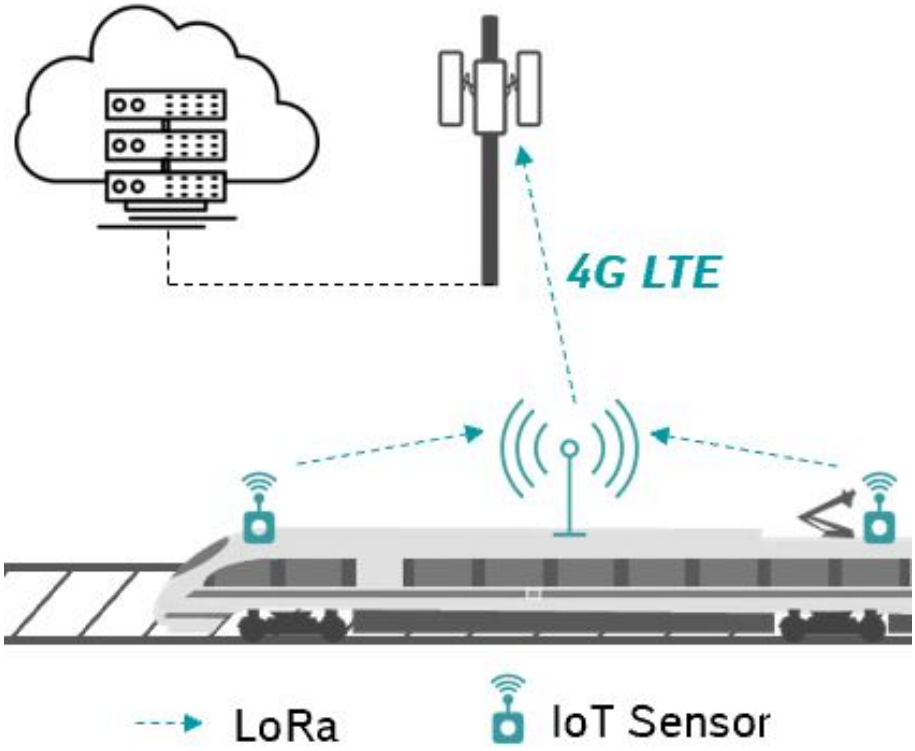

Figure 14 – Rolling stock equipment monitoring

Société nationale des chemins de fer français (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 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, sandbox monitoring, backup batteries state-of-charge monitoring, etc.

3.3.1 Safety Criticality

Regarding the Télédiag program, most of IoT systems deployed in rolling stock are not dedicated to critical applications and therefore can be classified as SIL 0.

3.3.2 Business Segment

The data collected can provide many services to several stakeholders:

- To a train operating company: operational center, train driver, train inspector, commercial staff, etc.
- To rolling stock maintenance depot: entity in charge of maintenance, maintenance agents, train owner, seller or repairer of spare parts, supply chain, etc.
- To the infrastructure manager: network maintenance engineering, monitoring and operational management, etc.
- To a product designer who gets data about rolling stock real behavior and to improve future hardware, etc.

3.3.3 Distinction from Conventional IoT

Because IoRT may be accessed by the public, SNCF has designed ruggedized IoT systems that can cope with regulatory requirements of railway. Each IoT sensor deployed must meet the EN 45545[12] and EN 50155[13] standards to ensure system safety. On the other hand, IoT protocols are based on COTS IoT components.

3.3.4 Security Impacts

IoT systems and information sent from train to ground must be protected and secured, typically by authentication and encryption. The cloud system must detect and be able to discard malicious data that could be sent by a fake IoT system. Eventually, some forensic analysis could be conducted. In any case, the identity and access right of each sensor must be protected as well.

3.3.5 IoT Model

Data Collection Each IoT system is made up of sensors that collect data about the state and the behavior of rolling stock machinery and equipment such as water level, doors, air conditioner state and so forth. The data is transmitted periodically through a LoRa radio interface.

Data Transmission Data collected by IoT systems is sent to the 3G/4G edge gateway using LoRa radio. Each packet sent to the gateway contains a unique identifier and the data gathered by the sensor. The gateway is equipped with a processing unit and two radio interfaces:

- LoRa radio interface is used for receiving data sent by IoT systems deployed in rolling stock.
- 3G/4G radio interface is used to transmit data collected from sensors to the cloud through public mobile network operators.

In the future, FRMCS could be used to transmit IoT data to the ground through a private network and frequency band such as 900 MHz or 1900 MHz.

Data Structuring The edge gateway is responsible for a first round of data analysis and structuring. Each data sent to the Cloud contains information gathered by the sensors and a timestamp. Data is then re-structured at the cloud side for analytics purposes.

[12]EN 45545: Railway applications – Fire protection on railway vehicles – Part 2: Requirements for fire behavior of materials and components

[13]EN 50155: Railway applications – Rolling stock – Electronic equipment

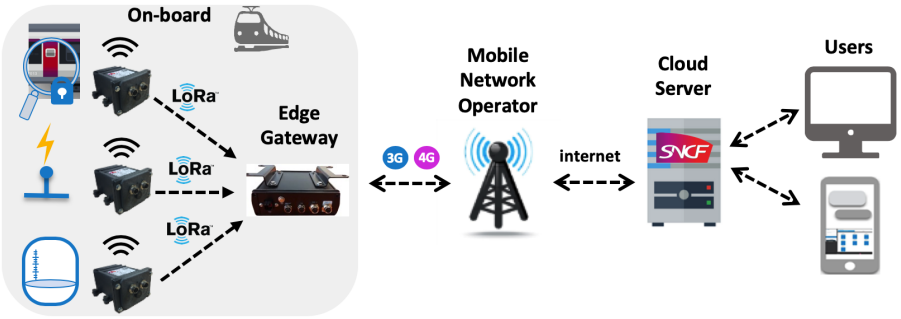

Figure 15 – Equipment monitoring and data transmission

Data Processing Two processing levels were implemented:

- On-board data processing: this part is responsible for analysing and extracting key information that could be sent to the Cloud.
- Cloud processing: this part is responsible for real-time data visualization and creating an alert summary that could be sent to maintenance agents.

3.4 Use Case 4: Monitoring Railway Level Crossings

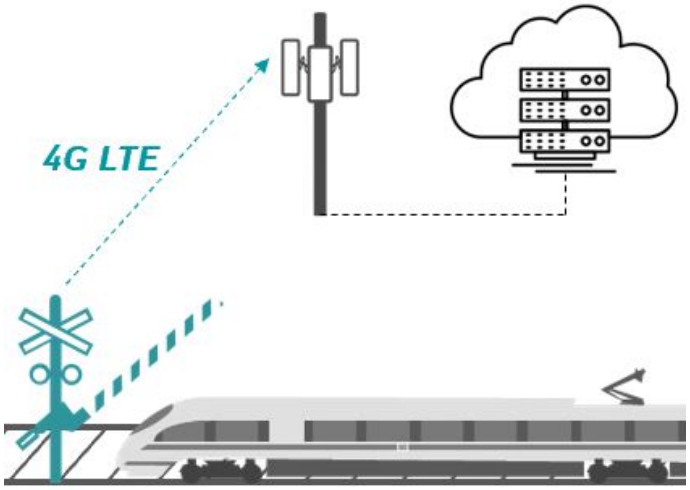

Figure 16 – Railway level crossing

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[14]. Thus, high level of safety is required for any rail level crossing.
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.

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

3.4.1 Safety Criticality

The information provided by the IoT system is only informative and can be classified as SIL 0. The IoT system have no impact on the level crossing safety or behavior.

3.4.2 Business Segment

Information provided by IoT systems can help early detection of defects or abnormal patterns in the behavior of the barrier. Such data could greatly enhance maintenance cycles and reduce collisions occurring at the crossing between cars and trains.

3.4.3 Distinction from Conventional IoT

Conventional IoT systems can deal with the first aim of the use case of monitoring the level crossing's operability. However, the second aim (vehicle impact and alert) requires handling stringent delay constraints in order to communicate with both the train driver and command and control center. Communicating with the train driver and command and control center may not use the same channel.

3.4.4 Security Impacts

IoT systems implemented in the barrier motors transmit highly sensitive data. Hence, it is very important to fully protect them against all kinds of attacks that could deny data availability, alter its integrity or simply its level of confidentiality.

3.4.5 IoT Model

The architecture of the monitoring system used is illustrated in Fig. 17.

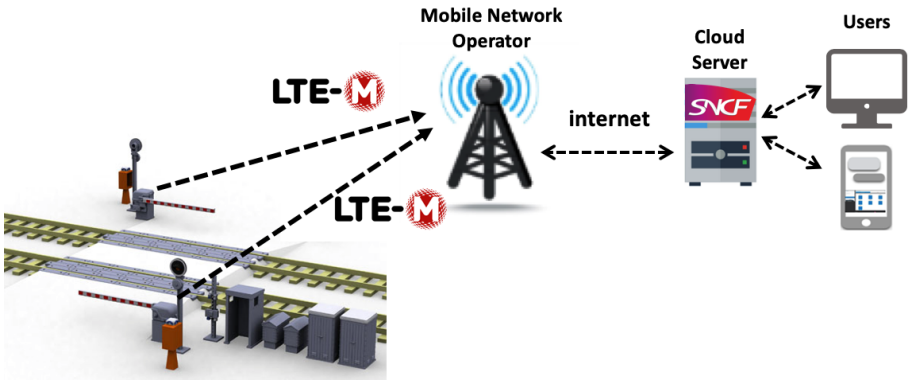

Figure 17 – Railway level crossing monitoring and data transmission

Data Collection Data collected by IoT system sensors is very simple and reflect the state of the crossing barrier or the health of the motor.

Data Transmission Data is transmitted through a public mobile network operator. Depending on network coverage, level crossing IoT systems could use a Long Range Wide Area Network (LoRaWAN) or an LTE-M radio interface to transmit the data to the Cloud.

Data Structuring IoT systems send periodically a packet containing the identifier of the railway crossing as well as the data collected by the sensors. Depending on the radio interface used, either LoRaWAN or LTE-M, a symmetric encryption could be applied to the packet sent to the Cloud.

Data Processing Most IoT systems send raw data to the Cloud which is responsible of packet decoding and data extraction. A processing is then applied in order to identify patterns and anomalies of the railway level crossing then take appropriate actions.

3.5 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.

4 Recommendations for a Secure IoRT

After exploring related work and 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.

4.1 IoRT Lifecycle

The railway IoT security requirements for devices in Section 4.2 and networks in Section 4.3 are structured along the IoRT lifecycle shown in Fig. 18. The lifecycle comprises the five phases *provisioning*, *deployment*, *operation*, *update*, and *decommission*. We explain the five phases in the following paragraphs.

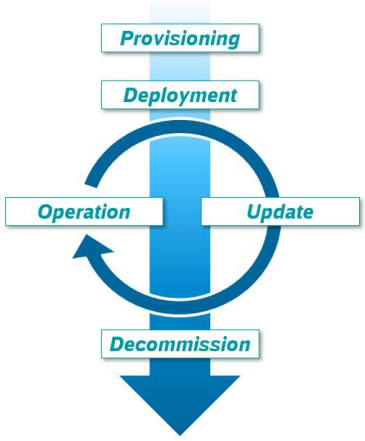

Figure 18 – IoRT Lifecycle

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.

Update A fundamental insight into security is that security is a process. The threat landscape of IT and 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.

4.2 Security for IoRT Devices

This section focuses on requirements and recommendations for IoRT devices.

4.2.1 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. This poses strong requirements towards hardware and physical security. Hardware, in which adversarial access can not be excluded, should be equipped with some form of tamper resistance, tamper detection (e.g. case opening alerts) or tamper evidence (e.g. seals, security fuses). 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). For further attestation of hard- and software, an IoRT edge device should employ authenticated or secure boot and a hardware-based root of trust that is used as anchor of a chain of trust that extends over the hardware and the various types of software running on the device. Based on the chain of trust, the operator can validate the running software's integrity during operation of the device and thus prohibit the execution of malware. Many cryptographic security applications rely on random numbers. A secure cryptographic random number generator can already be provisioned in hardware if necessary.

References: [10–12, 21, 26, 32, 33]

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. The limited capabilities of resource-constrained devices that are common in IoT can be reflected by the utilization of lightweight protocols and algorithms such as wolfSSL[15] or mbed TLS[16] which are specifically designed to operate on devices with limited resources.

References: [12, 36]

Reserve Resources for Updates The system resources should provide sufficient margins for updates. Software and security applications in particular require updates during the system's lifetime to remain secure. Cryptographic algorithms and key material might take up more resources due to the updates. Currently, increasingly faster processors available to break cryptographic keys are encountered with greater key sizes requiring more storage and CPU power. This arms race is

[15] `https://www.wolfssl.com/`
[16] `https://tls.mbed.org/`

likely to continue for some more years. 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.

References: [32, 36]

Manufacturer Provides Updates and Support Up-to-date devices – in particular software – 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.

References: [7, 18, 26]

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 [35].

References: [35]

4.2.2 Deployment

Remove or Change Default Credentials Many 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. Attackers can gain access to edge devices as well as virtually any device via default credentials. Many reports are available explaining security incidents where unauthorized access due to default credentials were involved. 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. The need to change default credentials is highlighted by an IoT worm called Silex programmed by a hacker claiming to be 14 years old[17]. Silex logged into Unix-based systems with default credentials and performed actions to effectively brick the device rendering it unusable.

References: [10, 12, 18, 21, 26]

Unique Credentials per Device Access credentials should be unique per device. The IoRT is particularly exposed to physical attacks as the use cases reveal. This paths the way for an attacker to eavesdrop credentials from network communication. Or worse, to get hold of a IoRT device and bypass every hardware protection demanded in Section 4.2.1 to exfiltrate the stored credentials. Unique credentials mitigate the effects of such an attack, because the attacker cannot gain advantage from the information as the credentials cannot be re-used to authenticate to a different device.

References: [10, 12, 21]

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. Some circuit boards provide debugging interfaces like JTAG or general purpose input/output pins that can be used to tamper with the

[17] `https://boingboing.net/2019/06/25/teenaged-kicks.html`

device. Less visible but similar widespread are wireless interfaces: Wi-Fi, Bluetooth, ZigBee, Cellular (GSM, GPRS, UMTS, 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.
Making physical ports unavailable reduces the attack surface of the device. Malware is often spread via USB sticks even to devices that are not connected to the public Internet or any network at all.

References: [10, 12, 18, 33]

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. Common services comprise remote access (secure shell (SSH), Telnet, RDP), web servers, web interfaces for configuration, maintenance, or monitoring as well as default file shares. 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.

References: [10, 12, 17, 26, 32]

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.

References: [12, 26, 32]

4.2.3 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. Cutting off the power supply is an attack vector as well that can be exploited to disguise unauthorized access if logs are not persisted without power.
Additionally, logs can be send to a logging server via protocols like syslog[18]. With a logging server, logs can be analysed centrally to detect incidents. Also, an attacker with physical access can not manipulate the logs after the fact on the device but not on a logging server. Depending on the power and memory resources of the edge device and the available network bandwidth, it is more beneficial to retrieve the logs on demand via remote access instead of pushing them to a server continuously. As any communication, the transmission of log messages should be authentic and confidential. When saved on edge devices or a logging server, logs should be protected from unauthorized changes to prevent disguising incidents in any case.

References: [12, 17, 18, 21, 32]

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

[18]RFC 5424 The Syslog Protocol `https://tools.ietf.org/html/rfc5424`

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. NIST SP 800-63B lists and explains the following authenticator types (among others) [29]:

- *Memorized Secrets*: Commonly referred to as passwords or PINs and the most widespread type of authenticator. Similarly, pre-shared keys are used to perform M2M authentication.
- *Look-Up Secrets*: A physical or electronic list of pre-shared secrets of which one secret is looked-up and presented for authentication. Most prominent examples are TAN lists that were frequently used to access online banking.
- *Out-of-Band Devices*: A physical device that can communicate via a secondary communication channel to authorize a user. Usually, to proof possession of the out-of-band device, the user needs to transfer an access token received on the primary channel to the device to be transmitted via the secondary channel or vice versa. This authenticator type is not suitable for M2M authentication.
- *one-time password (OTP) Devices*: Another proof of possession authenticator contrarily does not require secondary communication, because the access token is created cryptographically on the OTP device. A prominent examples are TAN generators. Small devices distributed by banks to their customers where bank cards can be inserted and authorization tokens for e.g. online banking are presented on the display.
- *Cryptographic Hard- and Software*: They securely store cryptographic keys in persistent memory (software) or on a dedicated device (hardware). The keys facilitate either symmetric or asymmetric cryptographic authentication schemes to proof the possession of the key to the opposite party. Prominent examples are X.509 certificates[19] and corresponding private keys used in public key infrastructures (PKIs), as well as the public and private keys used to authenticate an SSH session.

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. In the past, many password databases became public exposing the users' passwords that were not saved securely. Thus, passwords should not be re-used for authenticating on another device or service and should not appear in a public data breach to limit the effect of a breach. A well-known service to check passwords against their appearance in a breached database is *haveibeenpwned*[20], which also provides an application programming interface (API) to automate such a cross-check.
The BSI regularly publishes "Cryptographic Mechanisms: Recommendations and Key Lengths" [16]. A technical report with recommendations about key lengths sufficient for protection. The latest report at the time of writing (Nov 2019) is dated February 22, 2019.
Protection should be applied to prevent brute-force attacks that try to reveal credentials by (systematically) trying all possibilities. This applies to web interfaces, APIs, machine log-ins, as well as remote access like SSH. A common brute-force mitigation is rate limiting authentication attempts with reasonably increasing delay after consecutive failed logins. Literature does recommend an upper limit of failed login attempts, e.g. at 100 tries [21, 29]. Limiting to 100 attempts is far beyond any number a human would try to test a forgotten password. But the number is small enough to not offer an advantage to brute-force algorithms that need to try a far greater amount of passwords on average to succeed.
To further strengthen authentication, multiple authentication types can be combined to two factor authentication (2FA) or multi-factor authentication (MFA).

References: [12, 16–18, 21, 26, 29, 33]

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

[19] `https://tools.ietf.org/html/rfc5280`
[20] `https://haveibeenpwned.com/`

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.
Credentials such as passwords should be hashed and salted and only the resulting digest should be stored. During login the same hashing and salting is applied to the input and only the digests are compared to verify the credentials. A hash algorithm is a one-way function that efficiently maps an input (pre-image) to an output. However, the pre-image can not be recovered efficiently. A salt (a random bit string) is added to the input, because the same passwords would be hashed to the same digest otherwise. Same credentials in a large password database would be easy to spot if no salts were added. Recommendations on state-of-the-art hashing algorithms can be found in BSI's technical report [16].
Alternatively, credentials can be encrypted before storing them. For example, private keys of e.g. SSH keypairs or Transport Layer Security (TLS) certificates are typically protected with a symmetric key, a password. Dedicated secure storage and HSMs provide protection as well. HSMs provide APIs for de- and encryption such that cryptographic keys do not leave the protected hardware, an extra security measure.

References: [10, 12, 16, 26, 29]

Secure Storage for Data Similar to credentials, other sensitive or confidential data on edge devices should reside in encrypted storage [7]. 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.

References: [7, 10, 26]

Authorization Edge devices should employ an authorization model for actions to perform, data access and code to execute. An example is role-based access control (RBAC) for executing privileged actions. 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.

References: [7, 12, 26, 32]

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.

References: [16]

Safety and Reliability IoRT edge devices are exposed to tough environmental conditions such as varying temperature and humidity. The temperature sensors of the axle counter use case require line of sight vision on the axles to measure and must withstand high temperature in summer and low temperature in winter as well as sun, rain and snow.
On top of the fact that devices should be safe to use in any case, in a railway system, it is possible that the IoT adopts safety functions with which they interact with the physical world. For example as described in the axle counter with temperature measurement use case (see Section 3.1).
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. The following interruptions should be considered for edge devices:

- Loss of edge device's sensor or actuator function

- Loss of line power supply
- Loss of battery power supply
- Loss of wired or wireless network connection
- Loss of cloud server connection

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. In case the edge device cannot reach a cloud server anymore due to loss of connection or the server itself becomes unavailable, a standalone operation should be considered where the primary functionality of the edge device is maintained. In some cases however, this is not meaningful. As for example the axle counter use case (see Section 3.1) strongly depends on pushing the information about a hot axle towards the cloud. There is currently no alternative option to take action in case contact to the cloud is lost.
The edge device's sensor or actuator function cloud be lost as well. Such a malfunction could be caused by software bugs, failed updates, malware, ransomware, or loss of power (battery, line, or both). A prominent case in the media is a software glitch in an IoT thermostat draining the battery until the thermostat stopped working[21]. Eventually, rooms were not heated due to the out of order thermostats. The lesson to learn from this reports is that a manual way of operation should be provided for IoT actuators where applicable to prepare for such interruptions.

References: [7, 12]

Input Validation and Data Authentication A common entry point for malware and exploits are insecure 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. Typical examples of API or input level attacks are code injections (e.g. SQL) or malformed payloads to provoke buffer overflows or a denial-of-service (DoS). In general, a syntax check should be performed on incoming data and malformed data structures should be expected and accommodated for. Sensor data can be validated against a plausible range of values (e.g. temperature values in the axle counter use case) as a further semantic check on the data.
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 PKI and asymmetric cryptography.

References: [10, 12, 26, 32]

DoS Protection APIs exposed to the network can be subject to 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. [12].
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 (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

[21] `https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html`

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 [18].

References: [10, 12, 18]

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 [18]. But also APIs could be exploited to load malware on an IoT device [7].
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 [11] 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) [18]. 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 [18]. With removable media, even "airgapped" systems (i.e. systems without network connection) could be infected with malware. The most infamous example being Stuxnet.

References: [7, 11, 18]

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. The exclusion can be performed on network level with the help of a firewall by blocking all traffic to and from the device. If the identity of the device is bound to a digital certificate of a PKI, the certificate can be revoked. This implies that all devices in the IoRT system actually authenticate their communication and validate that the identity has not been revoked.

References: [21]

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.

References: [18, 21, 31, 36]

Secure Communication Although secure communications is a property for networks, the edge devices must support network security as well. This includes the support of TLS [12, 17, 18], VPN [17], and SSH [17].

References: [10, 12, 17, 18, 26]

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 ENISA's publication [11]. The most important tests are static analysis security testing, dynamic analysis security testing, fuzzing test and penetration testing.

References: [7, 11, 21]

4.2.4 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 3.3) 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.

References: [12, 26, 31]

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[22].

References: [10, 26]

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 [12].
Being able to roll-out updates over-the-air instead of having to be physically present at the device can significantly speed up the process and reduce cost. The use cases show that the devices to be updated can be at remote locations in the field that are not easy to access. In the rolling stock case, the over-the-air update could even be performed while the train is in operation, depending on the type and criticality of the sensor. Of course, remote updates assume the availability of respective network connection and bandwidth.
Digitally signing the update serves the purpose of disclosing alterations, irrespective of whether they are intentional by an attacker. Also verification of the signature ensures that only authorized entities can distribute and install updated software, such that no malicious update is installed.
It is important to assign the responsibility to provide an update in case of a vulnerability. Typically, this task is transferred to the manufacturer. However, if the manufacturer is unable to deliver the update (e.g. due to insolvency or non-existent legal contract) the device operator is left with an unpatched lot of devices if no precautions were taken.
ENISA recommends as well to have the devices check for updates automatically and install the update immediately once it becomes available. Automatic updates can simplify the process even further, because the update process is not started on each device. However, it should provide an option to be disabled as for example in use case 1, the update of the temperature sensor to detect

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

hot boxes, should only be performed while the track is not operational to avoid trains remaining unmonitored.
Oesterreichs Energie describes a secure update process for their smart meters in great detail [32]. It comprises digitally signing the firmware update and verifying the signature on the device before applying the update. The security properties and protection of the cryptographic key which is used for signing the firmware is described as well. Also, the public key on the devices can be exchanged by an authorized firmware updated. However, if the protection of the private key fails and it becomes compromised, the document does not discuss countermeasures for that case. An attacker knowing the public key could then roll-out signed firmware updates and even change the public key on the devices to something unknown to the actual owner, such that the owner can not restore the devices to an uncompromised version.

References: [7, 10, 12, 17, 21, 26, 32]

4.2.5 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 [7] what makes them quickly available for re-use. The 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 [27]. 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 [17].

References: [7, 10, 17, 26, 27]

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.

4.3 Security for IoRT Networks

This section focuses on requirements and recommendations for IoRT networks.
All modern railways heavily rely on communication networks and computer systems to monitor, control, and manage the physical machinery of railways operation. These communication networks can more or less easily be infected with all kind of malware, viruses, or attacked by a DoS attack. Hence, cyberattacks on railways is a real threat and few examples have been mentioned in Section 1.4. Communication networks in the railway domain are not enough protected and not fitted to the requirements in terms of security such as data confidentiality, data integrity, authentication of entities and service availability. In this section, we refer to Fig. 19, which represents all the aforementioned use cases. In our use cases presented in Sections 3.1 to 3.4, there are three main parts. The first one is represented by the objects or sensors along the rails (axle counter, temperature sensors or Fibre Optic Sensing), on the train (door state monitoring, water level monitoring in toilet tank, onboard seat occupancy monitoring) or on the ground (sensors to monitor the state of a level crossing barrier). The second one is the mobile network operator and the last one is the private cloud. The connected object is composed of the sensor, a memory, a battery and a radio frequency transmitter, a processor and an antenna. The gateway creates the connection between the local network and the control center on the private cloud.

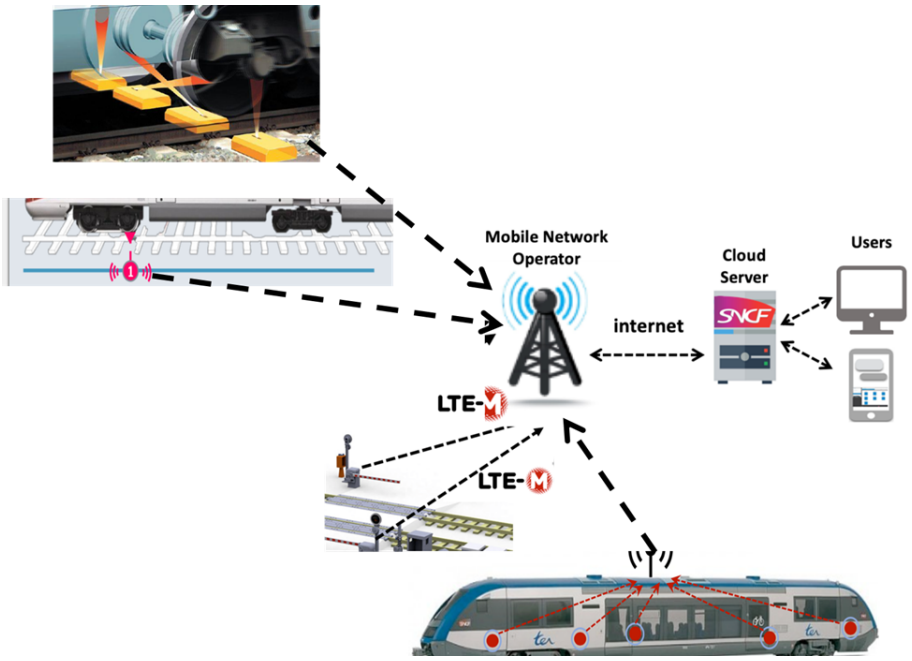

Figure 19 – Global use case conceptual view

In the following, we will discuss the security requirements, security protocols in theses networks along the IoRT lifecycle.

4.3.1 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 based on TLS or DTLS protocols, (2) an integration of a one time password mechanism in TLS or DTLS for device authentication and (3) a formal analysis of the proposed protocol through a tool such as Automated Validation of Internet Security Protocol and Applications (AVISPA) which investigates whether the target protocol is secure.

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 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 IIC, and several others. We briefly present some of these IoT standards and initiatives in Table 5

	802.11a	**802.11b**	**802.11g**	**802.11n**	**802.11 ac**	**802.11 ad**	**802.15.1**	**802.15.3**	**802.15.4**	**802.15.6**	**NFC**
Network Type	WLAN	WLAN	WLAN	WLAN	WLAN	WLAN	WPAN	WPAN	WPAN	WBAN	Point-to-Point
Date	1999	1999	2003	2009	2014	2012	2002/2005	2003	2007	2011	2011
Network Size	30	30	30	30			7	245	65535	250	-
Bit Rate	54 Mbit/s	11 Mbit/s	54 Mbit/s	248 Mbit/s	3.2 Gbit/s	$\geq$ 7 Gbit/s	3 Mbit/s	55 Mbit/s	250 kbit/s	10 Mbit/s	424 kbit/s
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5/60 GHz	2.4 GHz	2.4 GHz	868-915 MHz 2.4 GHz	402-405 MHz	13.56 MHz
Range	120 m	140 m	140 m	50 m indoor 250 m outdoor	30 m	5 m	100 m	100 m	75 m	2-5 m	0.2 m
Modulation	BPSK QPSK 16-QAM 64-QAM OFDM	DBPSK DQPSK CCK DSSS	DBPSK DQPSK 16-QAM 64-QAM OFDM	OFDM	OFDM	QAM-256	8DPSK DQPSK PIDQPSK GFSK AFM	QPSK DQPSK 16-QAM 32-QAM 64-QAM	ASK DSSS PSSS		Manschester and Modified Miller
Application	WiFi	WiFi	WiFi	WiFi			Bluetooth		ZigBee		

Table 5 – Main communication standards within IoT

Using these standards will establish trust in the manufacturer that the product has been developed with high communication, networks and security requirements.

Resources of IoRT devices The security protocols such as TLS, datagram transport layer security (DTLS) or SSH are used at the upper layers. However, in our use cases, the data transmitted by 4G or LoRa protocols are also encrypted at another layer. In fact, it is possible to encrypt these data by the application layer such as MQTT protocol or DTLS and encrypt them again at the link layer. During the provisioning process, attention should be paid that the performance could be reduced due to passing through several security levels.

4.3.2 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.
Possible attacks that may be mounted against IoRT system are presented hereafter.

- Manipulation of messages: modification or suppression of message fields (loss of information).
- Injection of false message: generate and send false information.
- Masquerade: posing as a legitimate node of the system.
- Replay: sending old messages.
- Eavesdropping and data analysis: listen to communication in order to collect and analyse information.
- Flooding: maliciously and artificially generating a high volume of false messages to disturb the network and equipment.
- Spamming: a high volume of messages introduced intentionally to increase the transmission latency and consume the bandwidth of network.
- Malware: introduction of malicious software.

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.

Use Secure Cipher Suites Several cipher suites must be preferred on TLS and VPN such as AEAD (Authenticated Encryption with Associated Data) cipher suites, PFS (Perfect Forward Secrecy) ciphers and all TLS 1.3 ciphers. As for encryption algorithm AES128-GCM, AES256-GCM and CHACHA20_POLY1305 must be preferred. In IoRT context, the ChaCha20 encryption algorithm is very fast in encryption and does not consume a lot of resources. For the key agreement protocol, ephemeral Elliptic Curve Diffie-Hellman (ECDHE) is highly recommended.

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 DTLS, only the version DTLS 1.2 should be used.

Change Default Configuration and Passwords During the setup, the default username and password on all devices or equipment must be changed. The default usernames and passwords initialized by the IoT vendors are available on the Internet. Some viruses are able to log into the device and infect it. During the deployment process attention should be paid that the sensors have a certificate to be authenticated or keys pre shared with the gateway.

Wireless Network Security Ensure that any access point is protected by the protocol WPA2-Enterprise 802.1X/EAP-PSK.

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.

4.3.3 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)
- OTP and SecureID Authentication Schemes

The majority of the schemes are dependent on the specific architecture of the IoT system. In addition, most of them require local key management and need infrastructure for storing keys, which makes them vulnerable to key thefts [24, 25, 34]. Most of them rely on a one-factor authentication scheme which can be a security risk in such an environment. One interesting authentication method fitted with the IoRT system is OTP. OTP is an authentication scheme in which a new password is generated for each authentication session and the reuse of a password is not possible. OTP is one of the most promising solutions for authentication in IoT [2, 34]. The OTP is a numeric code that is randomly and uniquely generated during each authentication event. This adds an additional layer of security, as the password generated is new each time an authentication is attempted. The standard for OTP is HMAC-Based One-Time Password (HTOP) as defined in RFC 4226. HTOP defines an algorithm to create a one time password from a secret key and a counter.

References: [2, 24, 25, 34]

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), MQTT, XMPP and several other protocols are used across the application layer with a security protocol.

4.3.4 Update

Monitor Vulnerabilities The CVE list is a public list of computer security vulnerabilities published by the MITRE Corporation in the USA. A CVE refers to the identifier of a security breach listed in this CVE list. The CVEs dissemination allows to prioritize and resolve vulnerabilities in the IoRT, thereby strengthening the security of these devices. Monitoring the updates of this list is among the security recommendations.

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.

4.3.5 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.

4.4 Connecting Use Cases and Requirements

To show the relation between the use cases and the presented requirements, Table 6 in the appendix 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.

4.5 Overview of References

Table 7 in the appendix gives an overview of the referenced documents for each listed requirement.

5 Reference Architecture

In this section, we synthesize and generalize the solutions sketched in the four use cases described in Section 3 to a common reference architecture and illustrate the application of the security requirements described in Section 4. It is not intended to go deep into technical details, but to provide the reader with key starting points in terms of security and data transmission. This reference architecture does not go along the totality of the seven layers as described in the Cisco reference model either (as illustrated in Fig. 1). Actually, the Cisco reference model is too high level and does not address security. Moreover, it does not detail enough the operational layers that are extremely important for the IoRT. However, it proposes an architectural structure in layers that is worth considering when building the system in a component-wise manner since they match with one technology and can help organising the project team or consortium. This being said, two key features must be seen globally in a cross layer manner: system management and security. Since they thoroughly fulfil their requirements only when considered in an end-to-end manner.

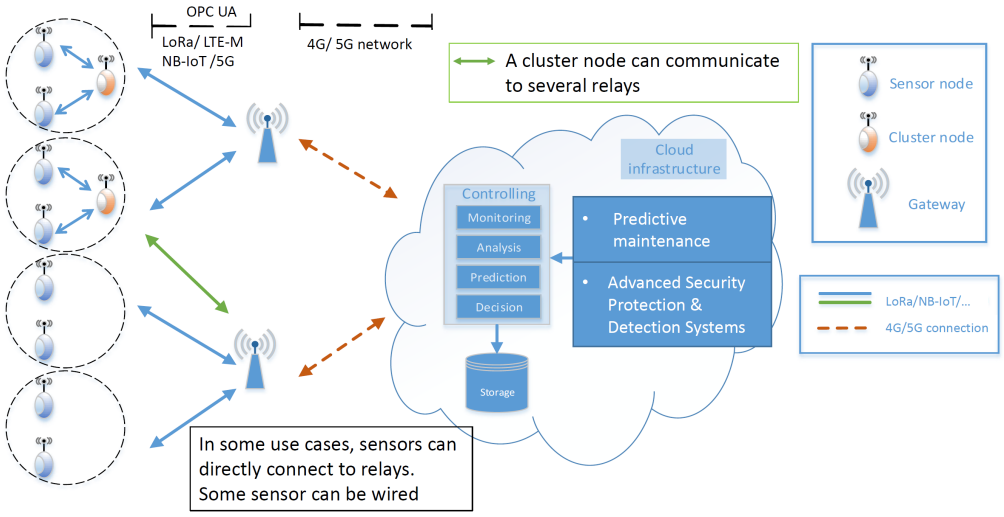

Figure 20 – Communication System Conceptual Architecture. Communication protocols such as LoRa, LTE-M, NB-IoT are used to bring data to the 4G/5G public network. Complex applications are processed remotely in a private cloud or a data center. Data is prepared on the edge: filtered, aggregated, cured, or compressed and encrypted then transmitted along the communication system.

The reference architecture does focus on the first layers of the Cisco model going from parameter measurements and data collecting through all kinds of sensors to securely transmit and store them in a private data center. Typical user applications such as the ones mentioned in the use cases (in particular predictive maintenance) are processed in the data center most likely private and are just mentioned in Fig. 20 and will not be described in details.
The four use cases are deployed along a large network of railway tracks or within numerous rolling stock vehicles. All of them are proceeding to measurements, collecting data. Most of them are comparing data to critical thresholds to be able to quickly send alerts. Then, collected data will be securely sent to a private cloud to be utilized typically in a command and control center. Later, they will be processed to derive potential optimizations or anomalies particularly for predictive maintenance purposes. The actual architecture of the private cloud is not scope of this document. Let us recall that today, computation can be performed just anywhere there is computational power, on the edge as mentioned in Fig. 22, but data can be aggregated or more generally processed in base stations as well. Accordingly, the reference architecture focuses mostly on the secured

information flow of measurement data from the sensors towards the IoRT data center where it can be further processed and create value for the railway company. As shown in Fig. 20, sensors can be clustered (for instance, for energy saving). Then, data can reach a first base station to enter in a public network and be transmitted to a data center. This constitutes a four layer architecture: data production, data transmission by a privately owned network, data transmission via a public network, data storage and processing. Sometimes, the public data transmission layer can be omitted, especially, when sensors are close to the storage location.
In the sequel, we first confirm and refine this view, starting from the use cases. Then, we go into more details in particular, with the communication protocol stacks according to a wired then to a wireless architecture.

5.1 Global View

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. Security requirements such as those described in Section 4.2 and Section 4.3 have to be taken into consideration. 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 4.2 and Section 4.3. 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.

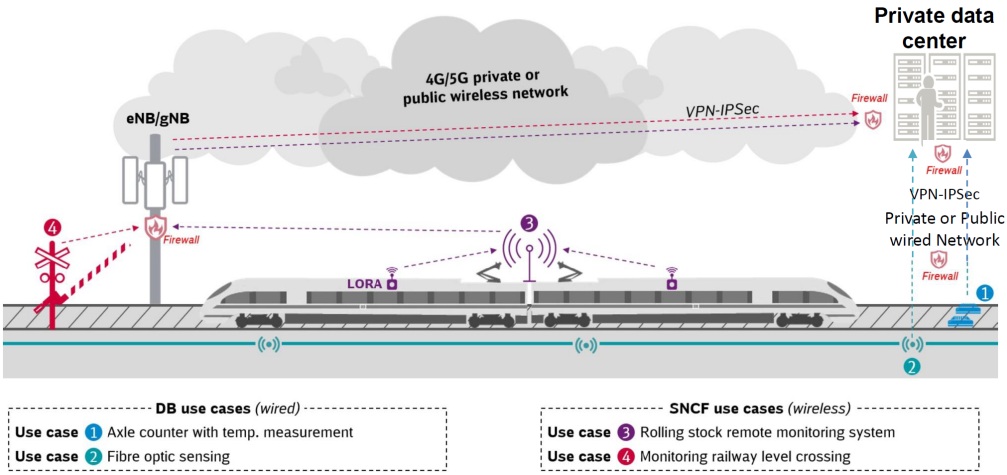

Figure 21 – Reference Architecture Global View. The four use cases are presented along the same railway track with a common data center, and two modes of communication: wired and wireless. eNB and gNB stand for base station, eNB (for evolved node B) interfaces with GSM or LTE while gNB (for next generation node B) interfaces with 5G. Message protection by VPN and IPsec have been seen in Section 4.3.2.

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 3.4. 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 (which may build up a double encryption), or at the entrance of the data center (here also, to build up a double protection). More sophisticated IDSs (see Section 4.3.2), protection, attack confinement, and recovery mechanisms must be available at the data center as hinted in Fig. 20. 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. For performance reasons, it is recommended not to use too many of them (Section 4.3.2). They can be more or less complex according to the criticality of the application and the intelligence required by the access policy.

The topology of the network as shown in Fig. 20 must be understood at a conceptual level and not at an actual level. The tree is showing the various sensors, modems, base stations, and other communication devices bringing data towards the data center. This tree essentially illustrates how data flows from the sensors to the data center. In the real world, the physical network will be more complex. There must exist several redundant routes to go from one point to another in order to avoid a single point of failure. There may be several data centers involved. However, this is strongly suggesting that the same kind of data will always go to the same storage lieu. The structure of a tree holds until we consider the possibility of a failure in the network or even in a physical data center in which case, data will have to be resend and rerouted.
On another hand, brokering or edge computation may create shortcuts in this structure and allow data when necessary to rapidly go from one node to another without necessarily transiting by a data center. Edge computing also can prepare and optimize data for transmission and efficient processing by transforming in various fashion and intents such as filtering, cleaning, curing, aggregating, or compressing.

At this point, it must be distinguished between wired and wireless architectures since they have very different behaviors and properties and different communication protocol stacks. In the cases of wired communications (use cases 1 and 2 in Fig. 21), a solution using OPC UA is sketched. In the cases of wireless communications (use cases 3 and 4 in Fig. 21), a solution with 5G and slicing is described.

5.2 Wired Architecture Features

The wired architecture is first presented in a conceptual manner where the four layers outlined in Fig. 20 are more detailed in Fig. 22. Second, a usage example of the OPC UA protocol as described in Section 2.3 is shown.
To protect the IoRT network against cyberattacks, it is important to establish end-to-end trust between the sensors and the data center represented by the "data protection" layers in the gateway and data center. The area labelled "public wired connection" in Fig. 22 is typically not under control of the IoRT operator such that only minimal assumptions about security should be made and security protection requirements apply. From a security perspective, the publicly operated

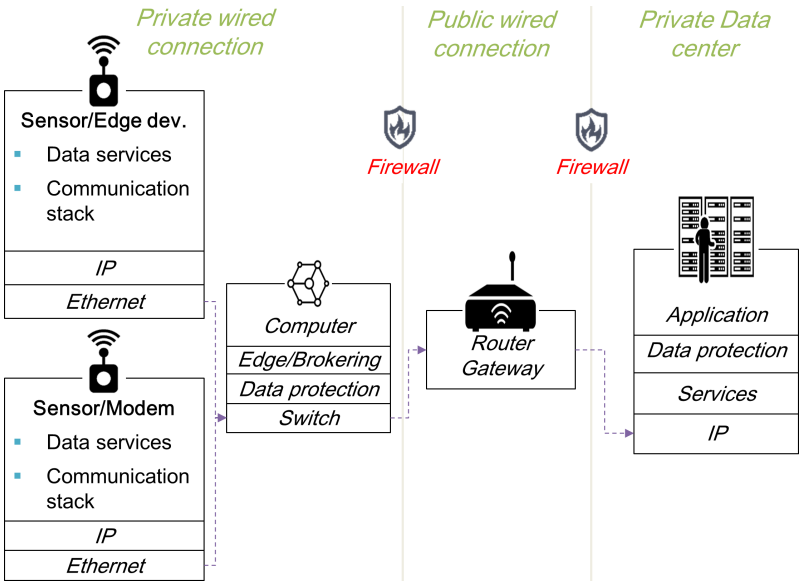

Figure 22 – Conceptual architecture with a wired communication. Data may have to go through a publicly operated network layer for cost effectiveness reason.

network should be treated as a black box that provides a service to transfer data between entities with limited security guarantees by the public network operator. Hence, the firewall at the entrance and the exit of the public network in order to ensure a required level of trustworthiness. By trustworthiness, we refer to the security goals of confidentiality and integrity. Sometimes, availability might be of importance to the use case and must be added to these security properties. This means that data travelling along the path from sensors to the data center can neither be modified nor be read by unauthorized persons. At the sensor layer, however, we are often dealing with limited resources (CPU power, power supply) in IoT and are forced to compromise between available resources and security protection. In some cases, we could be confronted with legacy devices that cannot be enhanced with security features. While it is desired to provide data protection beginning from the sensor, our reference architecture includes the case where a gateway device is the endpoint of end-to-end trust. The gateway aggregates data from associated sensors via less robust security protocols or – in case of need – without security protection at all. The use cases in Fig. 21 also show that sensors and modems could be connected to the public network directly without a gateway and thus need to operate secure communication themselves.
Firewalls should be placed at the borders between private (thus trusted) and public parts of the communication network to control the traffic flow crossing the borders and establish network segmentation (see Section 4.3.2). In case of the first layer IoRT of sensors, the gateway itself could assume the role of the firewall. In case of the last layer with the data center, this is typically a dedicated machine which will perform this function.
Figure 23 shows an example of an instantiation of the wired reference architecture Figure 22. The usage of TLS to establish secure communication between devices and the data center comes in addition to the security already provided by OPC UA and could very well be redundant. Many protocols are available today that provide security to various IoT use cases. Their choice depends on the required QoS, the environment including available resources, as well as assumed capabilities of the attacker. OPC UA seems to be a very promising one and already is in operation in the industry and has already been evaluated by both Deutsche Bahn (DB) and SNCF (see Section 2.3).
The protocols and other security measures need to be carefully selected for the concrete use case and evaluated for their cost, performance, and applicability in a real-world scenario.

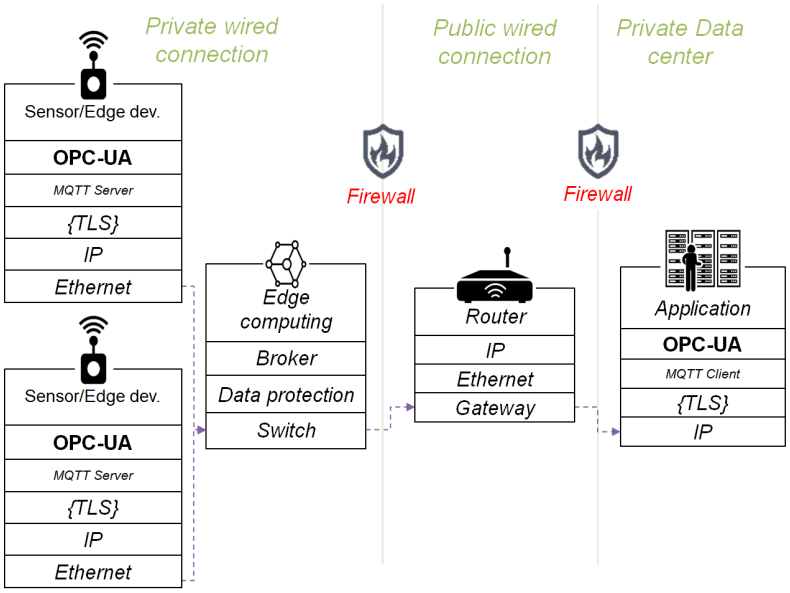

Figure 23 – Conceptual architecture with OPC UA and security protocols. Should you consider the level of security offered by OPC UA not sufficient, you still have the option to use TLS as an additional security layer.

5.3 Wireless Architecture Features

This section will detail the deployment of the two following railway use cases:

- Rolling stock remote monitoring use case
- Monitoring of railway level crossings

The first one is used to illustrate a 4G architecture, the second one a more recent, more complex, and more efficient 5G architecture. The two uses cases will have different constraints in terms of latency, jitter, throughput, transmission reliability, and security. These parameters are classical QoS ones and are at the source of technical choices. The wireless infrastructure will have to provide bearers that satisfy QoS constraints associated with the different uses cases.
In 4G networks, each application with specific QoS constraints will have a dedicated bearer allocated to it. This bearer is setup between the terminal and the Packet Data Gateway (PGW) (identified by an Access Point Name (APN)). As a result, a 4G infrastructure will have to ensure a dynamic sharing of all network resources between all active applications. 4G does not provide a way of allocating specific network resources to a given application or use case. 5G introduces this possibility by defining the *slicing concept*. An application running on top of a 5G infrastructure, will have access to specific logical resources along the transmission path between the terminal and the destination. Different slices will be isolated one from the other (data flows, computing and network resources). The slicing concept mainly relies on virtualization and NFV/SDN in the core network. Architecture and protocols of the Radio Access Network (RAN) have been modified to support slicing and being able to provide the same isolation property depicted above.
The two railway uses cases will be seen by the 4G network as two different bearers with specific QoS constraints. 5G will see these uses cases as two or rather three different slices since the railway level crossing use case necessitates two slices: one for critical real time data flow requiring both a high level of priority and a high level of security, and another one for data dealing with predictive maintenance applications.
The wireless architecture is described through three successive figures: a general one (Fig. 24), then Fig. 25 and Fig. 26 highlighting a few noticeable differences between a 4G and a more recent

5G architecture. In particular, we will depict slicing associated with the 5G architecture which responds to the need for supporting different types of signals with different level of confidentiality and priority.

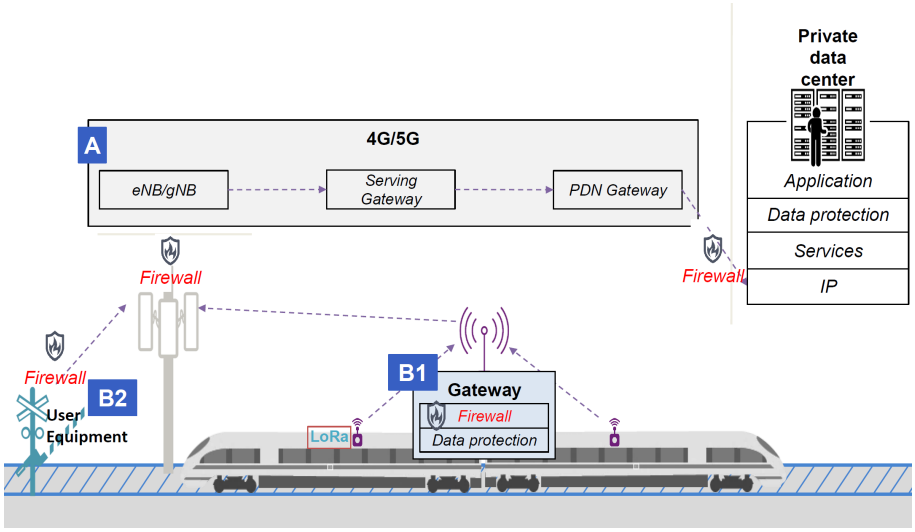

Figure 24 – Conceptual wireless architecture where use cases 3 and 4 from Fig. 21 are shown into more details. PDN stands for Packet Data Network, SGW is an acronym for Serving Gateway and PGW is an acronym for Packet Data Gateway. B1 communication protocol stack is detailed in Fig. 25 while B2 is detailed in Fig. 26.

In Fig. 24, the two wireless use cases are presented in slightly more detail compared to Fig. 21. The firewalls in Fig. 24 are now separating the sensor layer from the private communication layer, then again the public layer from the data center layer in a similar way than in the wired architecture. The areas labelled A, B1 and B2 are in turn detailed in the two following figures, the area B1 is being detailed in Fig. 25 with regard to the rolling stock use case using LoRa while the area B2 is being detailed with regard to the last use case.

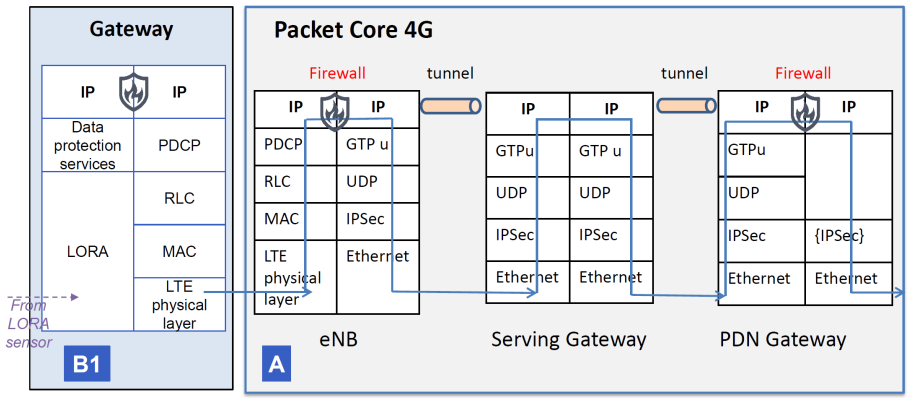

Figure 25 – Conceptual 4G architecture with an example of gateway LoRa-LTE-M from the rolling stock use case

Figure 25 and Fig. 26 utilize the following acronyms:

- PDCP = Packet Data Convergence Protocol is a protocol where ciphering and compression techniques can take place.

- RLC = Radio Link Control (LLC = logical link control would be used in the wired stack) is a link layer protocol that ensures transmission reliability by providing a selective repeat automatic repeat request (ARQ) scheme.
- MAC = Medium Access Control is in charge of scheduling radio resources on the air interface according to QoS constraints associated with different application flows.[23] It also provides the Hybrid ARQ functionality in order to speed up the error recovery process at the air interface level.
- GTP or GTPu = GPRS Tunneling Protocol, where GPRS = General Packet Radio Service, encapsulates the IP traffic originated/destined to final user. One GTP tunnel is associated per QoS user traffic profile.

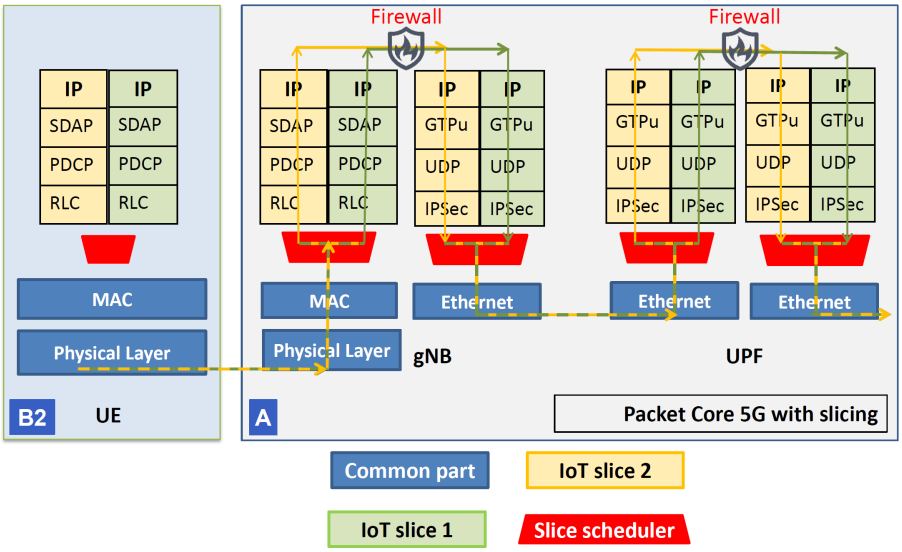

Figure 26 – Conceptual 5G wireless architecture with IoT isolation. SDAP stands for Service Data Adaption Protocol and UPF stands for User Plane Function, they are important modules of the 5G technology.

The blue line in Fig. 25 and the mixed yellow and green, yellow, and green lines in Fig. 26 are showing data flowing throughout the different protocols stacks, crossing the firewalls. Data is transmitted first by the mobile through the air interface. IP packets generated by the terminal are encapsulated in PDCP frames. PDCP frames are then ciphered before transmission on the air interface. The eNB receives the signals from the terminal and demodulate them to retrieve PDCP frames. Deciphering is consequently performed by eNB to retrieve IP packets sent by the terminal. eNB encapsulates the user IP packets in a GTP and UDP packet. IPsec performs ciphering of these content. The area A in Fig. 24 shows that eNB can then send the IPsec packet to the Serving Gateway (SGW), which will in turn decipher the information received to retrieve User IP packets. SGW will iterate the previous process to transmit data to the PGW. PGW will then transmit user data to the final destination using classical IP routing functionalities. If sensors use an IP private address, PGW must in this case operate Network Address Translation (NAT) translation. Otherwise, if IPv6 is used, no NAT is required at PGW level.

In 4G, the core network was designed to share network resources between several Service Data Flows (SDFs) potentially with different QoS profiles. SDFs are associated to one or several user IP flows. SDFs are in turn mapped on top of EPS bearers. EPS bearers basically gather network resources (e.g. GTP tunnels) and QoS profiles associated to them. 5G has introduced the concept

[23] MAC has another meaning, in Section 4.2.3 where it stands for message authentication code

of slicing and this changes the 4G paradigm by trying to dedicate virtual network elements to a specific type of application producing one or several IP flows. Figure 26 focuses on the 5G architecture and illustrates one possible deployment strategy of slicing between the MAC and the physical layers. Multiplexing of different slices allows to differentiate the traffic coming from different IP flows associated to different services (for example IoT slices for IoT, URLLC slice for V2x). One of the major security concerns regarding slicing will be the ability to grant isolation between slices instances running in different 5G network elements.

In Fig. 25, an example of a gateway from LoRa to LTE-M is shown. Other IoT technologies can be used as displayed in Table 3. The "data protection services" block is not a standard one and is an option that can perform encryption or detect and stop a cyberattack originating from a sensor. From the LTE-M network point of view, the LoRa-LTE-M gateway will behave as a terminal. As a result, it must be attached and successfully authenticated to the LTE-M core network before transmitting any information coming from sensors. End-to-end authentication procedures between the sensors and the applications located at the data center level are independent from those provided by the LTE-M network. In the rolling stock use case, we have many data connections going over a single mobile uplink where a single firewall could be responsible for protecting all communication entering and leaving the train that is considered a network segment of its own.

5.4 Concluding remarks on the reference architecture

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. It covers both wired and wireless technologies. In the case of wired communication, a solution using OPC UA is sketched. In the case of wireless communication, a solution with 5G and slicing is described. A rapid reading could conclude that each use case has its own architecture. That would be a too hasty conclusion. The security architecture is the same throughout the use cases. The communication protocol stacks that have been presented remain very similar relatively to their design and interconnection. Some IoT protocols differ relatively to the level of security they offer and their QoS capabilities. Benchmarking information such as presented in Table 3 can be useful to guide their choice with respect to comply with specific QoS requirements.
Actually, we believe that other IoRT use cases will be able to have a solution that complies with one or the other presented solutions and that this reference architecture can be used as a guideline for the design of future IoRT systems.

6 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 AI, IoRT is a key enabler for innovative and effective predictive maintenance applications. Eventually, it will foster the development of new products fully adapted to their applications. Combined with blockchains or distributed ledger technology, IoRT will allow to deal with the traceability of event chains across various independent partners, for instance in international freight transportation from one country to another with different regulations.

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 4.2 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 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
AMQP	Advanced Message Queuing Protocol
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	application programming interface
APN	Access Point Name
ARQ	automatic repeat request
AVISPA	Automated Validation of Internet Security Protocol and Applications
BSI	German Federal Office for Information Security
CAGR	compound annual growth rate
CoAP	constrained application protocol
COTS	commercial off-the-shelf
DB	Deutsche Bahn
DoS	denial-of-service
DPAS	Directed Path based Authentication Scheme
DTLS	datagram transport layer security
EC-GSM	Extended Coverage GSM
ENISA	European Union Agency for Cybersecurity
ERA	European Union Agency for Railways
FDD	Frequency Division Multiple Duplex
FOS	fiber optic sensing
FRMCS	Future Railway Mobile Communication System
HTOP	HMAC-Based One-Time Password
HSM	hardware security module
ICS	industrial control system
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
ISM	Industrial Scientific and Medical
IT	information technology
LoRaWAN	Long Range Wide Area Network
LoRa	Long Range
LPWAN	Low Power Wide Area Networks
LTE-M	LTE for Machines
LTE	Long-Term Evolution
M2M	machine to machine
MAC	message authentication code

MEMS	Micro-Electro-Mechanical Systems
MFA	multi-factor authentication
MQTT	Message Queuing Telemetry Transport
NAT	Network Address Translation
NB-IoT	Narrowband IoT
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
OFDMA	Orthogonal Frequency Division Multiplex Access
OPC UA	Open Platform Communication Unified Architecture
OPC	OLE for Process Control
OTP	one-time password
OT	operational technology
PDN	Packet Data Network
PGW	Packet Data Gateway
PKI	public key infrastructure
QoS	Quality of Service
RAN	Radio Access Network
RBAC	role-based access control
SCADA	Supervisory Control And Data Acquisition systems
SDAP	Service Data Adaption Protocol
SDF	Service Data Flow
SDLC	software development life cycle
SDN	Software Defined Networking
SGW	Serving Gateway
SIEM	security information and event management
SIL	safety integrity level
SNCF	Société nationale des chemins de fer français
SSH	secure shell
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Plattform Module
UML	Unified Modeling Language
UPF	User Plane Function
VPN	Virtual Private Network

List of Figures

List of Tables

Bibliography

[1] Agence Nationale de la Sécurité des Systèmes d'Information. Referentiels d'exigences, from 2010 to 2019. URL https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/.

[2] Adel Ali Ahmed and Waleed Ali Ahmed. An effective multifactor authentication mechanism based on combiners of hash function over internet of things. *Sensors*, 19(17):3663, 2019.

[3] BSI. Security Analysis by German Office for Information Security (BSI), 2019. URL https://opcfoundation.org/security.

[4] Francois Carrez. Internet of Things – Architecture Deliverable D1.5 – Final architectural reference model for the IoT v3.0. Technical report, IoT-A, 2013. URL https://iotforum.org/wp-content/uploads/2014/10/D1.5.pdf.

[5] Rodrigo Castiñeira and Andreas Metzger. The transformingtransport project, mobility meets big data. In *Proceedings of 7th Transport Research Arena TRA 2018, Vienna, Austria*, 2018.

[6] Marceau Coupechoux and Philippe Martins. *Vers les systèmes radiomobiles de 4e génération - De l'UMTS au LTE*. Collection IRIS. Springer, 2013. ISBN 978-2-8178-0084-4. doi: 10.1007/978-2-8178-0085-1. URL https://doi.org/10.1007/978-2-8178-0085-1.

[7] 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.

[8] George Corser et al. Internet of Things (IoT) Security Best Practices. Technical report, IEEE, 2017. URL https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf.

[9] K. Boeckl et al. Considerations for managing Internet of Things (IoT), cybersecurity, and privacy risks. Technical report, NIST, 2009. URL https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf.

[10] 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.

[11] 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.

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

[13] OPC Foundation. OPC Unified Architecture Specifications, Part 1 to Part 14, 2009-2018. URL https://opcfoundation.org.

[14] OPC Foundation. OPC UA Used in Deutsche Bahn Signaling System, 2015. URL https://opcconnect.opcfoundation.org/2015/06/opc-ua-used-in-deutsche-bahn-signaling-system.

[15] OPC Foundation. Practical Security Recommendations for Building OPC UA applications, 2019. URL https://opcfoundation.org/security.

[16] 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.

[17] 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.

[18] 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.

[19] Jim Green. The Internet of Things Reference Model. Technical report, CISCO, 2014. URL http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.

[20] GSM Association. CLP.11 – IoT Security Guidelines Overview Document. Technical report, GSMA, 2017. URL https://www.gsma.com/iot/iot-security/iot-security-guidelines/.

[21] 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/.

[22] International Electrotechnical Commission. IEC Guide 120 – Security aspects – Guidelines for their inclusion in standards. Technical report, IEC, 2017.

[23] Shi-Wan Lin, Mark Crawford, and Stephen Mellor. The Industrial Internet of Things Volume G1: Reference Architecture. Technical report, Industrial Internet Consortium, 2017. URL https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf.

[24] Chen-Xu Liu, Yun Liu, Zhen-Jiang Zhang, and Zi-Yao Cheng. The novel authentication scheme based on theory of quadratic residues for wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2013.

[25] Parikshit N Mahalle, Bayu Anggorojati, Neeli R Prasad, and Ramjee Prasad. Identity authentication and capability based access control (iacac) for the internet of things. *Journal of Cyber Security and Mobility*, 1(4):309–348, 2013.

[26] 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/.

[27] 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.

[28] National Institute of Standards and Technology (NIST). Systems security engineering. *Special Publication (NIST SP)-800-160 Volume 1*, 2016. doi: 10.6028/NIST.SP.800-160v1. URL https://doi.org/10.6028/NIST.SP.800-160v1.

[29] 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.

[30] National Institute of Standards and Technology (NIST). Developing cyber resilient systems: A systems security engineering approach. *Special Publication (NIST SP)-800-160 Volume 2*, 2019. doi: 10.6028/NIST.SP.800-160v2. URL https://doi.org/10.6028/NIST.SP.800-160v2.

[31] 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.

[32] 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.

[33] 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.

[34] VL Shivraj, MA Rajan, Meena Singh, and P Balamuralidhar. One time password authentication scheme based on elliptic curves for internet of things (iot). In *Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on*, pages 1–6. IEEE, 2015.

[35] 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.

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

[37] Martha Zemede. Explosion of the internet of things: What does it mean for wireless devices?, 2016. URL https://www.keysight.com/upload/cmc_upload/All/Explosion-of-the-Internet-of-Things.pdf.

A Connecting Use Cases and Requirements

To show the relation between the use cases and the presented requirements, Table 6 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** **Axle Counter**	**Use Case 2** **FOS**	**Use Case 3** **Rolling Stock Monitor**	**Use Case 4** **Level Crossing**
Provisioning	Hardware Security	Edge Device Temperature Sensor Cloud Server	Light Sensor Processing Unit Storage 4G Modem Cloud Server	Sensors LoRa Interface Edge Gateway 3/4G Modem Cloud Server	Electric Sensor Radio Interface Cloud Server
	Resources for Security	Edge Device	Processing Unit	(Sensors) Edge Gateway	Radio Interface
	Reserve Resources for Updates	Edge Device	Processing Unit	Edge Gateway	Radio Interface
	Manufacturer Provides Updates and Support	Edge Device Temperature Sensor Cloud Server	Light Sensor Processing Unit 4G Modem Cloud Server	Sensors LoRa Interface Edge Gateway 3/4G Modem Cloud Server	Electric Sensor Radio Interface Cloud Server
	Product Security Certification	Edge Device Cloud Server	Processing Unit 4G Modem Cloud Server	LoRa Interface Edge Gateway 3/4G Modem Cloud Server	Radio Interface Cloud Server
Deployment	Remove or Change Default Credentials	Edge Device	Processing Unit 4G Modem	LoRa Interface Edge Gateway 3/4G Modem	Electric Sensor Radio Interface
	Unique Credentials per Device	Edge Device	Processing Unit 4G Modem	LoRa Interface Edge Gateway 3/4G Modem	Radio Interface
	Remove or Block Unnecessary Physical Interfaces	Edge Device	Processing Unit 4G Modem	Sensors LoRa Interface Edge Gateway 3/4G Modem	Radio Interface
	Disable Unnecessary Services	Edge Device Cloud Server	Processing Unit Storage 4G Modem Cloud Server	Sensors LoRa Interface Edge Gateway 3/4G Modem Cloud Server	Radio Interface Cloud Server
	Secure Interfaces, APIs and Services	Edge Device Cloud Server	Processing Unit Storage 4G Modem Cloud Server	Sensors LoRa Interface Edge Gateway 3/4G Modem Cloud Server	Radio Interface Cloud Server
Operation	Logging	Edge Device	Processing Unit	Sensors Edge Gateway	Radio Interface
	Strong Mutual Authentication	Edge Device Cloud Server	Processing Unit (4G Modem) Cloud Server	LoRa Interface Edge Gateway 3/4G Modem Cloud Server	Radio Interface Cloud Server
	Secure Storage for Credentials	Edge Device	Processing Unit 4G Modem	LoRa Interface Edge Gateway 3/4G Modem	Radio Interface

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

Table 6 – Mapping Use Case Assets to Requirements

B Overview of References

Table 7 gives an overview of the referenced documents for each listed requirement.

	Requirement	BITAG IoT Security and Privacy Recomm. [7]	ETSI TS 103 645 [10]	ENISA Good Practices for Security of IoT [11]	ENISA Good Practices for IoT Tool [12]	BSI Cryptographic Mechanisms [16]	BSI IT Baseline Protection: SYS 4.4 [17]	BSI ICS Security Top 10 [18]	GSMA CLP.13 [21]	OWASP IoT Top 10 [26]	NIST Guidelines for Media Sanitization [27]	NIST Digital Identity Guidelines [29]	NIST Framework [31]	Oesterreichs Energie [32]	IIC IIoT G4: Security Framework [33]	IACS Cybersecurity Certification Framework [35]	Resilient Architectures in Railway Signalling [36]
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 7 – 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