



Analysis of Security in Railway 5G Communication Networks for Cyber and Physical Intrusions

Tiago José Pinto Figueiredo

Thesis to obtain the Master of Science Degree in
Telecommunications and Informatics Engineering

Supervisors: Prof. Dr. Luís Manuel de Jesus Sousa Correia
Prof. Dr. Ricardo Jorge Fernandes Chaves

Examination Committee

Chairperson: Prof. Dr. Fernando Manuel Valente Ramos

Supervisor: Prof. Dr. Ricardo Jorge Fernandes Chaves

Members of Committee: Prof. Dr Miguel Filipe Leitão Pardal

: Eng. Fernando Manuel Lopes Santana

June 2025

I declare that this document is an original work of my own authorship and that it fulfils
all the requirements of the Code of Conduct and Good Practices of the
Universidade de Lisboa.

To my friends and family.

Acknowledgements

This master's thesis marks an important achievement in my academic and personal journey, and it would not have been possible without the support of many people who, in different ways, contributed to its completion.

First, I would like to express my sincere gratitude to Professors Luís Correia and Ricardo Chaves for their guidance, availability, and invaluable advice throughout this process. Above all, I am grateful for the time and attention they devoted to supporting me.

I extend my thanks to Eng. Fernando Santana, Eng. Tiago Costa and Eng. Nuno Frigolet from HITACHI, whose collaboration, feedback, and technical discussions provided important insights that enriched this thesis.

A special thank you to my family, for their endless support, encouragement, and for instilling in me the values that have guided me to this point.

To my friends, thank you for the moments of friendship, understanding, and celebration that accompanied this long road. You have all been an important part of my life.

Finally, to all those who, directly or indirectly, contributed to my growth and learning, my most sincere thanks.

Thank you!

Abstract

This thesis analyses security vulnerabilities in railway communication networks using 5G technologies. The study focuses on both physical and cyber threats affecting the base station, the mobile terminal, and the train's internal communication systems. A top-down methodology was used, applying the STRIDE framework for threat identification and the DREAD model for risk evaluation. Components were grouped logically and physically to reflect different attack surfaces. The base station was found to be highly resilient to cyber-attacks but vulnerable to physical denial of service, with attacks classified as medium risk. The mobile terminal emerged as a critical point of failure, where denial of service attacks could cause major operational delays. Inside the train, switches and gateway servers located in the driver's cabin were identified as the most valuable targets, with successful attacks leading to severe operational and financial damage. Attacks on components in the passenger carriages were easier to perform but initially had lower impact unless used to pivot to critical systems. Risk reduction measures such as motion detection alarms, traffic inspection barriers, and IP layer encryption were proposed to mitigate vulnerabilities. An alternative train architecture based on distributed gateways was analysed and found to increase attack surfaces significantly, making it less secure than architectures based on physical segregation. The methodology developed proved adaptable and can be applied to future railway communication standards. Overall, the results show that while 5G security features, such as mutual authentication, encryption of user data, and subscription identity protection, improve resilience, careful architectural design and layered protections remain essential to secure railway operations.

Keywords

Railways, Communications, Cybersecurity, 5G, Security Evaluation, Risk Assessment

Resumo

Esta dissertação analisa vulnerabilidades de segurança em redes de comunicação ferroviária baseadas em tecnologias 5G. O estudo foca-se em ameaças físicas e cibernéticas que afetam a estação base, o terminal móvel e os sistemas de comunicação internos do comboio. Foi utilizada uma metodologia top-down, aplicando o modelo STRIDE para identificação de ameaças e o modelo DREAD para avaliação de riscos. Os componentes foram agrupados logicamente e fisicamente para refletir diferentes superfícies de ataque. A estação base revelou-se altamente resiliente a ataques cibernéticos, mas vulnerável a ataques físicos de interrupção de serviço, sendo estes classificados como de risco médio. O terminal móvel destacou-se como um ponto crítico de falha, onde ataques de interrupção de serviço poderiam causar atrasos operacionais significativos. No interior do comboio, os switches e servidores gateway localizados na sala do maquinista foram identificados como alvos de maior valor, com ataques bem-sucedidos a causarem graves danos operacionais e financeiros. Os ataques a componentes nas carruagens de passageiros são mais fáceis de executar pelo atacante, mas inicialmente com menor impacto, a menos que sejam usados para escalar a ataques a sistemas críticos. Foram propostas medidas de mitigação de riscos, como alarmes de deteção de movimento, barreiras de inspeção de tráfego e encriptação ao nível da camada IP. Foi também analisada uma arquitetura alternativa baseada em gateways distribuídos, tendo-se concluído que esta aumentava significativamente as superfícies de ataque, tornando-se menos segura do que arquiteturas baseadas em segregação física. A metodologia desenvolvida demonstrou ser adaptável e poderá ser aplicada a futuros padrões de comunicação ferroviária. Os resultados mostram que, embora as funcionalidades de segurança do 5G, como a autenticação mútua, a encriptação dos dados do utilizador e a proteção da identidade do utilizador, aumentem a resiliência, uma arquitetura de rede bem planeada e proteções em várias camadas continuam a ser essenciais para garantir a segurança das operações ferroviárias.

Palavras-chave

Ferrovia, Comunicações, Cibersegurança, 5G, Avaliação de Segurança, Análise de Riscos

Table of Contents

Acknowledgements	vii
Abstract.....	ix
Resumo	x
Table of Contents.....	xi
List of Figures	xiii
List of Tables.....	xiv
List of	xv
List of Software	xviii
1 Introduction	1
1.1 Overview and Motivation.....	2
1.2 Objective and Structure	4
2 Background.....	5
2.1 Mobile Communications Concepts.....	6
2.1.1 GSM and GSM-R.....	6
2.1.2 5G	9
2.2 Cybersecurity	12
2.2.1 General Concepts	12
2.2.2 Threat and Risk Modelling	15
2.2.3 Security in Communications	16
2.3 Security in 5G	18
2.3.1 Security Architecture.....	18
2.3.2 Authentication	19
2.3.3 Privacy	20
2.3.4 Attacks and Countermeasures	20
2.4 Services and Applications	23
2.5 Railway Communications.....	25
2.5.1 Railway Network	25
2.5.2 Services and Applications.....	26
2.5.3 Security in Railway Communications.....	28
2.6 Related Work	30

2.7	Chapter 2 Summary.....	32
3	Railway Architecture	33
3.1	Railway Services.....	34
3.2	General Railway Architecture	35
3.3	Control Centre Architecture	37
3.4	Train Architecture.....	38
3.4.1	Train's General Architecture	38
3.4.2	Services with Physical Segregation.....	41
3.4.3	Services without Physical Segregation.....	43
3.5	Base Station Architecture	44
3.6	Chapter 3 Summary.....	45
4	Security Assessment and Mitigation	47
4.1	Security Analysis Flow for Railways.....	48
4.2	Security Assumptions	49
4.3	Attacker Model.....	50
4.4	Vulnerable Entry Points	51
4.5	Security Evaluation	52
4.5.1	Security Analysis Classification Methodology	52
4.5.2	Security Evaluation: Base Station.....	55
4.5.3	Security Evaluation: Mobile Terminal	61
4.5.4	Physical Security Evaluation: Train	65
4.5.5	Cyber/Logical Security Evaluation: Train.....	68
4.5.6	Security Evaluation: Attacker's Perspective	72
4.6	Risk Reduction.....	75
4.6.1	Risk Reduction: Base Station	75
4.6.2	Risk Reduction: Train	76
5	Conclusions	79
5.1.1	Conclusions	81
5.1.2	Limitations.....	82
5.1.3	Future Work	83
	Annex A. 4G Onboard Communication System.....	85
	References.....	87

List of Figures

Figure 1.1 – Global average weekly attacks by industry 2022 compared to 2021 (extracted from [1]).	2
Figure 2.1 – Allocation of frequencies in the 900 MHz band (extracted from [10]).	7
Figure 2.2 – GSM-R system architecture (extracted from [9]).	7
Figure 2.3 – 5G architecture overview (extracted from [17]).	9
Figure 2.4 – NSA architecture (extracted from [17]).	9
Figure 2.5 – SA architecture (extracted from [17]).	10
Figure 2.6 – 5G SA's complete architecture (extracted from [18]).	11
Figure 2.7 – Public-key cryptography (extracted from [24]).	13
Figure 2.8 – Extensible Authentication Protocol (extracted from [27]).	14
Figure 2.9 – Simplified network diagram.	16
Figure 2.10 – ESP in transport mode.	17
Figure 2.11 – Security architecture (extracted from [36]).	19
Figure 2.12 – SUPI structure and concealed sensitive information (extracted from [38]).	20
Figure 2.13 – Example of some attacks against a 5G network (extracted from [39]).	21
Figure 2.14 – 5G key features (extracted from [42]).	24
Figure 2.15 – General railway architecture.	26
Figure 2.16 – GSM-R voice services (extracted from [44]).	26
Figure 3.1 – Railway services.	34
Figure 3.2 – General railway architecture.	36
Figure 3.3 – Railway control centre architecture.	37
Figure 3.4 – Train architecture.	39
Figure 3.5 – Simplified control room architecture.	40
Figure 3.6 – Train's physical architecture with a focus on physical segregation.	42
Figure 3.7 – Logical architecture with physical segregation.	42
Figure 3.8 – Train's physical architecture with a focus on logical segregation.	43
Figure 3.9 – Logical architecture without physical segregation.	44
Figure 3.10 – 5G base station architecture.	44
Figure 4.1 – Security framework for railways.	48
Figure 4.2 – Physical and cyber-attack entry points for a 5G railway network.	52
Figure 4.3 – Tree of Threats for the base station.	56
Figure 4.4 – Scenarios for physical attacks against a base station.	57
Figure 4.5 – Scenarios for cyber-attacks against a base station.	58
Figure 4.6 – Tree of Threats for the Mobile Terminal	61
Figure 4.7 – Scenarios for physical attacks against the MT.	62
Figure 4.8 – Scenarios for cyber-attacks against the MT.	63
Figure 4.9 – Tree of Threats for the train's components.	65
Figure 4.10 – Scenario for physical attack on the components inside the driver's cabin.	66
Figure 4.11 – Scenario for physical attack on the components inside the passenger's carriage.	66
Figure 4.12 – Filtering component to prevent malicious packets arriving at the driver's cabin.	77
Figure A.6.1 - Onboard communication system's topology used by HITACHI in Chile's trains.	86

List of Tables

Table 2.1 – Some attacks and their countermeasures (adapted from [39]).	23
Table 2.2 – Performance requirements for railway scenarios (extracted from [45]).	28
Table 2.3 - Timeline of cybersecurity incidents in the railway sector (adapted from [46]).	29
Table 3.1 – Critical service requirements and specifications.	35
Table 4.1 – Attacker’s capabilities	51
Table 4.2 – Scoring criteria for DREAD risk assessment categories.	54
Table 4.3 – STRIDE table for the Base Station.	55
Table 4.4 – Physical attack on base station: damaging/destroying the components of the BS.	58
Table 4.5 – Cyber-attack on base station: radio jamming.	59
Table 4.6 – Attacker bypasses access control system.	60
Table 4.7 – STRIDE table for the Mobile Terminal.	61
Table 4.8 – Cyber-attack on the MT: flooding with excessive connections.	63
Table 4.9 – Cyber-attack on the MT: malware injection.	64
Table 4.10 – STRIDE table for the train’s components.	65
Table 4.11 – Physical attack on the driver’s cabin: destroying/damaging the switch.	67
Table 4.12 – Physical attack on the passenger carriage: destroying/damaging the switch.	67
Table 4.13 – Cyber-attack on the Gateway Server on the driver’s cabin: traffic injection.	68
Table 4.14 – Cyber-attack on the Gateway Server on the passenger carriage: traffic injection.	69
Table 4.15 – Cyber-attack on the driver’s cabin switch: traffic injection.	70
Table 4.16 – Cyber-attack on the passenger’s carriage switch: traffic injection.	70
Table 4.17 – Cyber-attack on the Control and Signalling terminal: MitM attack.	71
Table 4.18 – Cyber-attack on the CCTV terminal: MitM attack.	71
Table 4.19 – Attacker’s perspective: Base Station.	72
Table 4.20 – Attacker’s perspective: Mobile Terminal.	73
Table 4.21 – Attacker’s perspective: Physical attack on switches.	73
Table 4.22 – Attacker’s perspective: Cyber-attack on gateway servers.	74
Table 4.23 – Attacker’s perspective: Cyber-attack on switches.	74
Table 4.24 – Attacker’s perspective: Cyber-attack on service terminals.	75

List of Abbreviations

5G	Fifth Generation
5GC	5G Core Network
AMF	Access and Mobility Management Function
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ARPF	Authentication credential Repository and Processing Function
AUSF	Authentication Server Function
BS	Base Station
BSC	Base Station Controller
CC	Control Centre
CCSW	Control Cab Stand-Alone Switch
CCTV	Closed-Circuit Television
CN	Core Network
CR	Control Room
CSW	Cab Stand-Alone Switch
CIA	Confidentiality, Integrity, Availability
DN	Data Network
DoD	Denial of Defence
DoS	Denial of Service
DREAD	Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability
EAP	Extensible Authentication Protocol
eMLPP	enhanced Multi-Level Precedence and Pre-emption
eNB	Evolved Node B
EN-DC	E-UTRAN and NR Dual Connectivity
ERTMS	European Railway Traffic Management System
ESP	Encapsulating Security Payload
ETCS	European Train Control System
E-GSM-R	Extended GSM-R
FR1	Frequency Range 1
FR2	Frequency Range 2
FRMCS	Future Railway Mobile Communication System
GS	Gateway Server
GSM	Global System for Mobile Communications
GSM-R	Global System for Mobile Communications – Railway
HDTV	High-Definition Television
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISC	Interlocking System Centre

LTE	Long Term Evolution
ME	Mobile Equipment
MFA	Multi-Factor Authentication
MIMO	Multiple Input Multiple Output
MSC	Mobile Switching Centre
MS	Mobile Station
MT	Mobile Terminal
NAS	Non-Access Stratum
NEF	Network Exposure Function
NG	Next Generation (Interface)
NG-RAN	Next Generation Radio Access Network
NMS	Network Management System
NSA	Non-Stand-Alone
NSACF	Network Slice Admission Control Function
NSS	Network Switching System
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PCM	Pulse Code Modulation
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RSA	Rivest-Shamir-Adleman
SA	Stand-Alone
SDN	Software-Defined Networking
SEAF	Security Anchor Function
SHA-256	Secure Hash Algorithm 256-bit
SIDF	Subscription Identifier De-Concealing Function
SIM	Subscriber Identity Module
SMF	Session Management Function
SCP	Service Communication Proxy
SSS	Switching Subsystem
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TS	Train Station
UE	User Equipment
UDM	Unified Data Management
UDR	Unified Data Repository
UIC	International Union of Railways
UPF	User Plane Function
URLLC	Ultra-Reliable Low-Latency Communications
USIM	Universal Subscriber Identity Module
VGCS	Voice Group Call Service
VBS	Voice Broadcast Service

VPN Virtual Private Network
WiFi Wireless Fidelity

List of Software

Microsoft Word	Document editing
ChatGPT	Grammar and text correction
Grammarly	Grammar and text correction
Draw.io	Diagram creation

Chapter 1

Introduction

Chapter 1 introduces the thesis, focusing on the challenges faced by railway communication systems due to cyber threats and the need for improved security measures. It outlines the transition from the older GSM-R system to advanced technologies like 5G. The structure and objectives of the thesis are also presented, detailing the approach towards achieving a secure communication framework for railways.

1.1 Overview and Motivation

In recent years, cyber-attacks have become a serious threat to infrastructure systems, including those used in railway networks. As society increasingly depends on these systems, they become attractive targets for malicious actors. Cybercriminals, hacktivist groups, and state-sponsored attackers often target critical infrastructure to disrupt services, obtain sensitive information, or cause financial and reputational damage. Data from 2022 shows a notable increase in attacks across all sectors, with transportation and energy being among the affected [1].

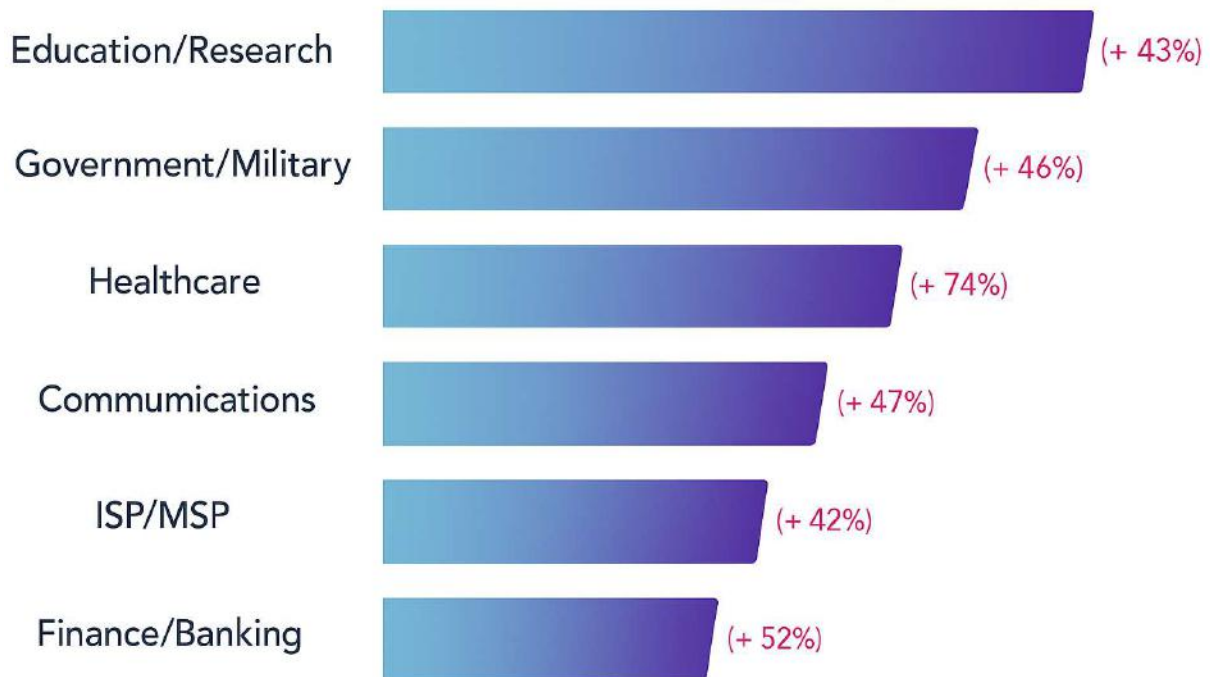


Figure 1.1 – Global average weekly attacks by industry 2022 compared to 2021 (adapted from [1]).

Figure 1.1 shows that most of the most targeted institutions are the educational and research institutions, with an average of 2,314 attacks per week per organisation, an increase of more than 40% from 2021. Although these sectors are highly targeted, railway networks are also facing more frequent attacks due to the growing use of digital systems and remote communication technologies. Modern railway networks rely on many connected components spread over large distances, such as base stations, control centres, and equipment inside trains. This wide and open structure makes them especially vulnerable to both cyber and physical attacks. The 2008 Lodz tram incident in Poland [2], in which a teenager derailed several trams through a homemade remote-control device, and the 2021 attack on Iran's railway system [3] are stark reminders of how physical and digital vulnerabilities can intersect.

In the realm of railway operations, secure and reliable communication networks are not just a technological requirement but a cornerstone of safety and efficiency. This thesis delves into the critical need for comprehensive security analysis in the railway communication systems, particularly as they undergo a significant technological transition. While the European railways have predominantly relied on the GSM-R system, a 2G+ based framework established over three decades ago by the International

Union of Railways (UIC) [4], the evolving landscape of cybersecurity threats and operational demands calls for a shift towards more advanced technologies like 5G.

GSM-R, integral to the European Railway Traffic Management System (ERTMS) and spanning over 130,000 kilometres of track in Europe and approximately 210,000 kilometres globally, has reached a juncture where its aging infrastructure is increasingly susceptible to cyber and physical intrusions [5]. The move to modern technologies like 5G offers faster, more secure networks with greater capacity. But this change is more than a simple upgrade; it involves challenges like the large scale of current GSM-R systems and the strict demands of railway communications.

The Future Railway Mobile Communication System (FRMCS) [6] is an upcoming global standard for railway communication, set to replace the existing GSM-R technology. FRMCS is based on 5G technology and is designed to meet the needs of modern rail operations, including high-speed data communication, increased reliability, and support for a range of new applications such as automated trains, advanced traffic management, and multimedia services for passengers. The FRMCS specifications will provide the framework for implementing a unified, secure, and efficient communication system that supports interoperability across different countries and rail networks. In the meantime, projects such as 5GRAIL [7] are being developed to meet these specifications and make the transition from GSM into 5G possible.

However, the transition to 5G introduces new challenges. Railway communication environments are characterised by long hardware lifecycles, strict certification requirements, and coexistence with legacy systems. Additionally, the 5G architecture increases the number of potential attack surfaces due to its distributed structure and the rise in connected devices. These developments require a careful reassessment of existing security practices, and the implementation of robust protection mechanisms tailored to the railway domain.

This thesis focuses on analysing the cybersecurity implications of adopting 5G in railway communication networks. Specifically, it examines the communication link between trains and base stations, and the internal structure of the base station and train systems. The problem under study is the identification of cyber and physical vulnerabilities introduced or amplified by the shift to 5G, and the development of targeted mitigation strategies to ensure safe and continuous operation of railway services.

To carry out this analysis, this work applies two structured methodologies: the STRIDE framework, which classifies potential threats into categories, and the DREAD model, which supports risk assessment by evaluating threats based on multiple impact factors. These methods are used to examine key components of the railway communication system, such as the train architecture, base station, and the communication links between them. The analysis includes the identification and classification of possible physical and cyber entry points into the system, considering different attacker profiles and capabilities. Based on this evaluation, a set of mitigation strategies is proposed to address the most relevant threats, considering both technical effectiveness and implementation feasibility.

The innovative aspect of this thesis lies in its practical and systematic approach to security analysis in the context of railway networks adopting 5G technologies. By combining established threat modelling

and risk assessment techniques and applying them to the specific context of railway communications, the work aims to provide a structured methodology to guide future security planning and system design.

1.2 Objective and Structure

The objective of this thesis is to analyse security threats in railway communication systems operating over 5G networks. The focus is on identifying vulnerabilities that may arise from both cyber and physical attack vectors and evaluating how these threats impact critical components of the railway system. In addition, the thesis aims to assess the adequacy of existing security mechanisms and, where necessary, propose countermeasures to mitigate the most relevant risks and strengthen the overall resilience of the system.

The thesis is organised into five chapters, as follows:

- Chapter 1 provides the overview, motivation, objectives, and the structure of the work.
- Chapter 2 introduces key concepts in mobile communications (GSM, GSM-R, and 5G), general and 5G-specific cybersecurity principles, and the use of communication systems in railways. It also summarises relevant related work in this field.
- Chapter 3 describes the railway communication system under analysis, including its key components such as the control centre, base station, and train. It also details the physical and logical structure of the network and classifies services based on criticality and security relevance.
- Chapter 4 presents the developed security framework and analyses threats using the STRIDE and DREAD models. It defines attacker profiles, identifies vulnerable entry points, and evaluates risks across various system components. The chapter concludes by proposing mitigation strategies adapted to each threat.
- Chapter 5 summarises the key findings, reflects on the limitations of the current analysis, and proposes directions for future research to improve railway cybersecurity in 5G environments.

Chapter 2

Background

Chapter 2 provides an overview of the essential background knowledge necessary for understanding the thesis. It covers key concepts in mobile communications, including GSM, GSM-R and 5G and delves into cybersecurity principles. This chapter discusses the evolution of mobile communication technologies, their applications in railway systems, and some security challenges associated with each. At the end of the chapter, the Related Work section provides information about recent work being done in the field of 5G networks in railways.

2.1 Mobile Communications Concepts

This section delves into the technical aspects of mobile communication systems relevant to railway communications, specifically GSM and GSM-R and 5G. It outlines the evolution and characteristics of each technology, explaining their roles and implementations in the context of modern communication networks. It discusses the transition from GSM to more advanced systems like 5G, which offer significant improvements in terms of speed, capacity, and security.

2.1.1 GSM and GSM-R

Introduced in the early 1980s, GSM, or Global System for Mobile Communications [8], emerged as the first standardised digital cellular network, revolutionising the way people communicate globally. Before GSM, mobile communication systems were characterised by a lack of standardisation, making interoperability between different networks and devices challenging. The introduction of GSM addressed this issue by establishing a unified set of standards for mobile communication.

One of its key contributions was the shift from analogue to digital technology. This transition significantly improved voice quality, reduced interference, and paved the way for the integration of data services. This was possible using Pulse Code Modulation (PCM) and Time Division Multiple Access (TDMA). PCM converts analogue voice signals into a digital format which ensures the accurate representation of voice, reducing distortion and improving overall quality. TDMA divides radio frequency into time slots, allowing multiple users to share the same frequency without interference which results in an increased network capacity.

GSM also played a crucial role in enhancing the security of mobile communication. The implementation of digital encryption mechanisms in GSM made it more resistant to eavesdropping and unauthorised access, addressing privacy concerns associated with earlier analogue systems. GSM employs the A5 family of encryption algorithms to secure voice communication between mobile devices and the network. Also, a session key is generated for each voice call. This session key is unique to the specific call and is not reused. The key generation process involves a combination of the Mobile Station (MS), the Subscriber Identity Module (SIM) card, and the network's Authentication Centre.

GSM-R, or Global System for Mobile Communications-Railway, is a specialised wireless communication standard designed for railway operations. It is an extension of the GSM standard, tailored to meet the specific needs of the railway industry. GSM-R was chosen as the communication technology for railways due to its established use in commercial networks and the cost-efficiency it offered for adaptation to railway requirements.

Dedicated base stations (BSs) are installed beside the railway track to configure the GSM-R system. The distance between any two neighbouring BSs is different from country to another depending on the local environment, for instance, it is from 3 to 5 km in China and 7 to 15 km in Europe [9]. The cell range or the area covered by each BS is around 8 km, and the frequency band used by GSM-R system is around 900 MHz. However, there are extra frequency bands used in GSM-R on a national basis known

as extended GSM-R (E-GSM-R). These frequency bands are 873 to 876 MHz and 918 to 921 MHz, the former is for up-link and the latter is for down-link, shown in Figure 2.1.

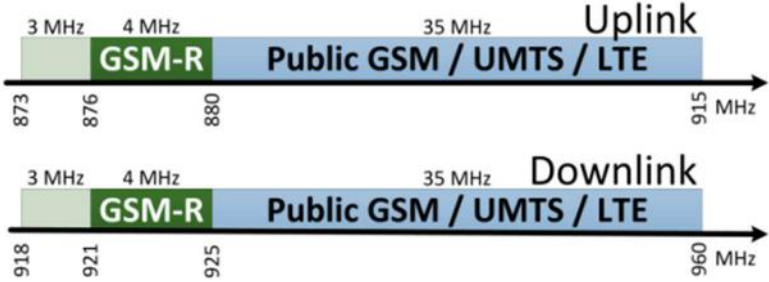


Figure 2.1 – Allocation of frequencies in the 900 MHz band (extracted from [10]).

The BSs are linked together in groups and controlled by base station controller (BSC). This BSC also provides the connection between the BSs and the mobile switching centre (MSC). The MSC is one of the mobile switching subsystems (SSS). The MSC is the network core which is responsible of the connection between the users of the system and managing the mobility of the users. Furthermore, its gateway oversees connecting between the GSM-R network and other public networks. This architecture can be seen in Figure 2.2.

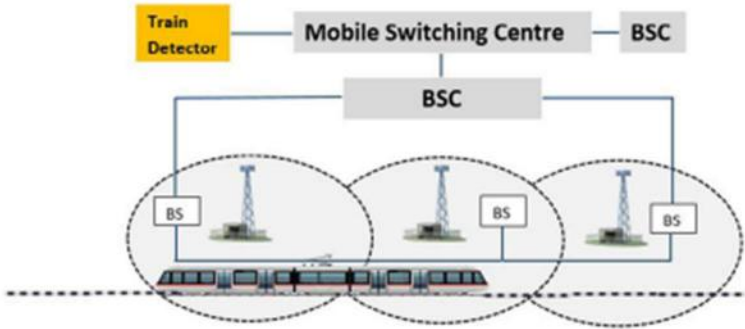


Figure 2.2 – GSM-R system architecture (extracted from [9]).

The European Telecommunications Standards Institute (ETSI) [11] specified additional services for GSM-R [12] [13] [14] such as Voice Group Call Service (VGCS), that enables simultaneous communication among a defined group of users, Voice Broadcast Service (VBS), a service designed for broadcasting voice messages, and enhanced Multi-Level Precedence and Pre-emption (eMLPP), a feature that provides enhanced priority handling for certain communication sessions based on predefined levels of precedence and pre-emption. In railway scenarios, where critical communications related to safety and control take precedence, eMLPP ensures that these communications receive priority over less urgent ones. Also, GSM-R is integrated with railway signalling systems, enabling features like the European Train Control System (ETCS), which requires high reliability and low latency communication for safe train operations. The ETCS is a component of the ERTMS that standardises railway signalling equipment and procedures to enhance cross-border interoperability and safety across the European railway network [15]. It operates at various levels, each facilitating different degrees of communication and supervision between trains and trackside. Level 1 allows for continuous train movement supervision with non-continuous communication, typically through Eurobalises (electronic

beacons or transponders placed on railway tracks), while Level 2 enhances this with constant communication for continuous supervision, making lineside signals optional. Level 3 further integrates train location and integrity management within the ETCS, eliminating the need for lineside signals or external train detection systems. Additionally, Level 0 and Specific Transmission Module (STM) cater to trains on non-equipped lines or requiring interfacing with national systems. ETCS also encompasses various operational modes, including Full Supervision and Automatic Driving, adapting to the operational status of onboard and trackside equipment.

Despite its significant contributions to mobile communication, GSM-R does have some shortcomings [10]. In Europe, GSM-R operates in a dedicated 4 MHz frequency band. While GSM-R is deployed in more areas, it becomes apparent that interference caused by public operators, using the neighbouring band, is an issue. The problem increases because both railway and commercial operators want to have as good coverage as possible along the tracks, so they interfere with each other, instead of cooperating during network planning. Also, the allocated 4 MHz band for GSM-R, imposes capacity limitations, potentially hindering its ability to support advanced applications, especially those requiring continuous data connections, such as the ETCS Level 2. ETCS Level 2 is an advanced train control system that relies on continuous data connections for real-time monitoring and control of trains. The system requires frequent and uninterrupted data exchanges between trains and control centres to ensure precise and up-to-date information on train positions, speeds, and conditions.

Also, with the development of technology some issues have arisen:

- The A5/1 encryption algorithm used in GSM-R is known to have vulnerabilities, and it operates on a relatively short key length (64 bits) [10]. This makes it susceptible to cryptographic attacks, such as brute force or rainbow table attacks, where an adversary could potentially decipher the encryption and eavesdrop on sensitive communications.
- Base stations and infrastructure are often located in proximity to railway tracks for optimal coverage. However, this physical accessibility makes them susceptible to tampering, vandalism, or unauthorised access. Attackers could potentially compromise the equipment, disrupt services, or gain unauthorised control.
- As per the analysis conducted on GSM-R [16], it has been identified that the GSM-R protocols lack end-to-end encryption. This implies that while the wireless link between Mobile Stations (MS) and Base Stations (BS) is encrypted, the information transmitted between different Base Stations (BS to BS) is done in clear text. Furthermore, GSM-R adopts a one-way authentication approach, where the network (BS) authenticates the Mobile Station (MS) during access attempts, but the same level of authentication is not reciprocated when the Base Station (BS) communicates with the Mobile Station (MS). This one-way authentication creates a vulnerability, enabling potential active attacks that could efficiently steal information within the GSM-R network by impersonating a false Base Station (BS), ultimately leading to network instability or collapse.

4G Core Network. In the NSA architecture, the (5G) NR base station (logical node "en-gNB") connects to the (4G) LTE base station (logical node "eNB") via the X2 interface. The X2 interface was introduced prior to Release 15 to connect two eNBs. In Release 15, it also supports connecting an eNB and en-gNB to provide NSA. The NSA offers dual connectivity, via both the 4G AN (E-UTRA) and the 5G AN (NR). It is thus also called "EN-DC", for "E-UTRAN and NR Dual Connectivity".

Unlike 5G NSA, SA represents a fully independent and end-to-end 5G network architecture whose objective is to deliver an array of services and features, surpassing the capabilities of its predecessors. The SA architecture, Figure 2.5, can be seen as the "full 5G deployment", not needing any part of a 4G network to operate. The NR base stations (logical node "gNB") connect with each other via the Xn interface, and the Access Network (called the "NG-RAN for SA architecture") connects to the 5GC network using the NG interface.

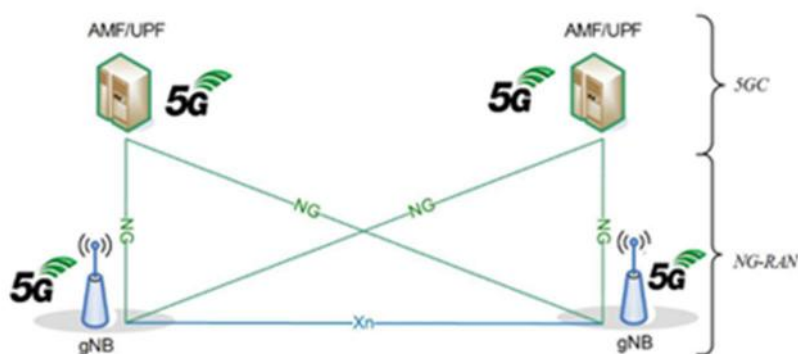


Figure 2.5 – SA architecture (extracted from [17]).

A more detailed SA architecture is shown in Figure 2.6. It consists of the following network functions and entities:

- NSSF (Network Slice Selection Function): Selects the appropriate network slice for the user.
- NEF (Network Exposure Function): Exposes capabilities of the network to other network functions or third-party applications.
- NRF (Network Repository Function): Supports service discovery and maintains information about network functions.
- PCF (Policy Control Function): Manages policy control decisions.
- UDM (Unified Data Management): Handles user data and subscription information.
- AF (Application Function): Enables applications to interact with the core network and influence traffic routing.
- EASDF (Edge Application Server Discovery Function): responsible for the discovery of edge application servers.
- NSSAAF (Network Slice-specific and SNPN Authentication and Authorisation Function): Handles authentication and authorisation for network slicing.
- AUSF (Authentication Server Function): Manages authentication of users accessing the network.
- AMF (Access and Mobility Management Function): Responsible for all access and mobility

management tasks.

- SMF (Session Management Function): Manages the sessions within the network.
- SCP (Service Communication Proxy): serves as an intermediary that facilitates communication between different network functions.
- NSACF (Network Slice Admission Control Function): Manages the admission control for network slicing.
- UE (User Equipment): Device used by the end-user to access the network.
- RAN (Radio Access Network): Part of the network that connects the UE to the core network.
- UPF (User Plane Function): Routes and forwards user data packets.
- DN (Data Network): External networks connected to the 5G system (e.g., the internet or corporate networks).

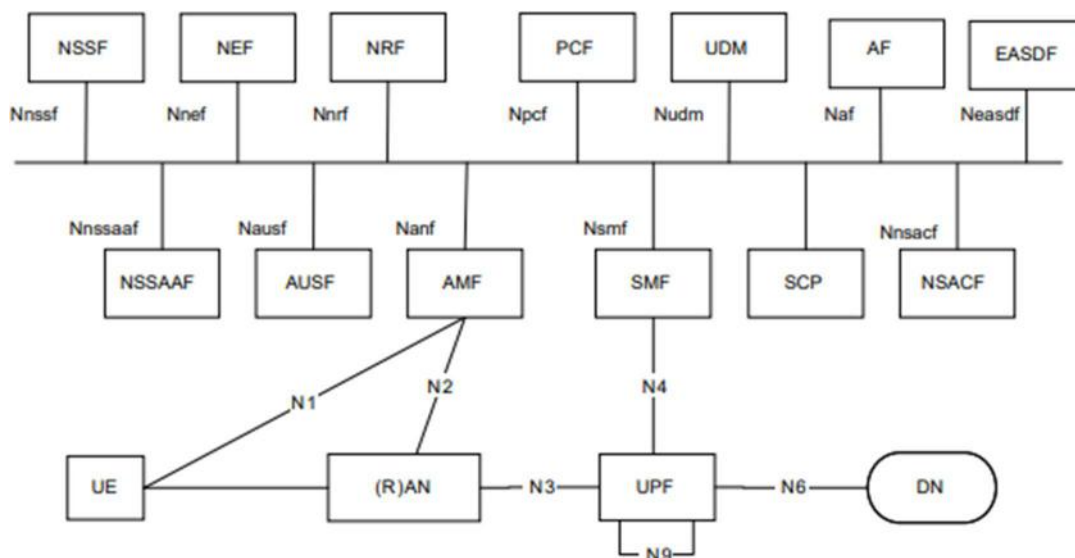


Figure 2.6 – 5G SA's complete architecture (extracted from [18]).

More detailed information about the 5G architecture and its components can be found on many ETSI technical specification reports [18].

Additionally, 5G incorporates advanced radio technologies, with Massive Multiple Input Multiple Output (MIMO), network slicing and EDGE computing standing out as key features.

Massive MIMO enables the simultaneous transmission of multiple data streams, leading to improved coverage and a reduction in interference.

EDGE computing means that some computational power is introduced as "physically close" to the end-user as possible. Some applications like virtual reality, factories of the future or autonomous driving, are very demanding in terms of the propagation's/network's response time. To reduce this time, some "local replications" of a main server are introduced closer to the end-user.

The concept of network slicing is described as partitioning a physical network into several virtual networks, each optimised for a specific type of application or subscriber [19]. This is made possible through advancements in computing and network function virtualisation (NFV) technologies. Network

slices can provide tailored services for distinct application scenarios, offering flexibility and customisation over the same network infrastructure. According to the definition in [20], network slicing consists of three layers:

- Service Instance Layer: Represents the end user services or business services that can be supported. Each service is represented by a service instance.
- Network Slice Instance Layer: Includes the network slice instances that can be provided. A network slice instance provides the network features that are required by the service instance.
- Resource Layer: Provides all virtual or physical resources and network functions that are necessary to create a network slice instance.

Network slicing is enabled by some key technologies like virtualisation, software-defined networking (SDN) and management/orchestration.

2.2 Cybersecurity

This section provides an overview of cybersecurity principles critical for protecting communication technologies used in railway systems. It introduces general concepts of cybersecurity, including the basics of encryption and data integrity and threat and risk modelling.

2.2.1 General Concepts

Cybersecurity involves protecting computer systems, networks, and data from unauthorised access, attacks, or damage. It includes implementing various technologies, practices, and processes to safeguard systems and sensitive information from cyber threats.

Cybersecurity basics revolve around three core principles often referred to as the CIA properties [21] [22]. These principles are:

- Confidentiality: ensures that information is only accessible to authorised individuals or systems and is protected from unauthorised access. The goal is about maintaining privacy and keeping sensitive data concealed.
- Integrity: ensures the accuracy and trustworthiness of data. It verifies that data remains intact and unaltered during storage, transmission, or processing. Unauthorised or accidental changes to data should be prevented.
- Availability: ensures that information and systems are consistently accessible when needed. This involves preventing disruptions, downtime, or denial of service attacks that could render systems or data unavailable.

There are many ways and tools to achieve these principles such as encryption, hashes, and intrusion detection systems (IDS).

Encryption is a process of converting readable, plaintext data, into unreadable, ciphertext data, using an algorithm and a cryptographic key [23]. The algorithm applies mathematical operations to the

plaintext, and the key influences the transformation. Only someone with the corresponding decryption key can reverse the process, turning the ciphertext back into the original plaintext. There are two main types of encryptions, asymmetric and symmetric. The asymmetric encryption, Figure 2.7, also known as public-key cryptography [24], involves the use of a pair of keys: a public key for encryption and a private key for decryption. These keys are mathematically linked, where the public key can be shared openly to encrypt messages, while the private key is kept secret by the owner and used to decrypt messages. Notable examples of asymmetric encryption algorithms include RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and DH (Diffie-Hellman).

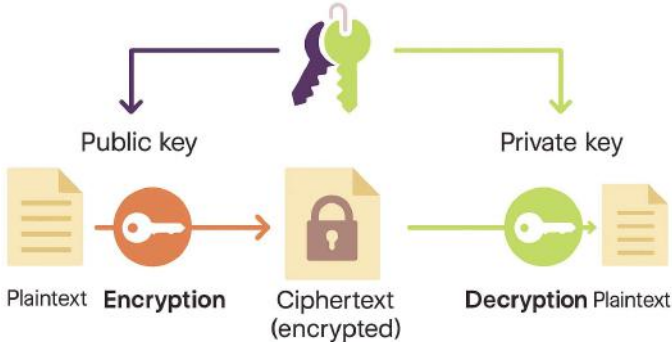


Figure 2.7 – Public-key cryptography (adapted from [24]).

Symmetric encryption is a method of encryption where the same key is used for both encrypting and decrypting the data. This means that both the sender and the recipient of the encrypted message must share the same key to encrypt the data before sending and then decrypt it upon receipt. The key is a secret that should be protected since anyone with access to it can decrypt the data. This encryption method is fast and efficient, making it suitable for encrypting large volumes of data. It is widely used in various security protocols and systems for securing data both in transit and at rest. AES (Advanced Encryption Standard), used in 5G communications, is an example of a symmetric encryption algorithm.

A hash function is a mathematical algorithm that takes an input (or message) and produces a fixed-size string of characters [25]. Hashes are deterministic, which means that the same input will always produce the same output, and are irreversible, meaning that it should be computationally infeasible to reverse the process and derive the original input. A widely used cryptographic hash function is SHA-256 (Secure Hash Algorithm 256-bit). When data is created or received, a hash function is applied to generate a fixed-size hash value based on the content of the data and that value is stored. At a later point, when the integrity of the data needs to be checked, the hash function is applied again to the current state of the data. The newly generated hash value is compared to the originally generated hash value, if they match, it means indicates the data has not been altered, if it doesn't match, then that data was tampered with.

An IDS is a network security solution designed to monitor, detect, and prevent malicious activity [26]. It works by analysing network and/or system activities for signs of known threats or abnormal behaviour and takes action to block or mitigate those threats. It examines data packets to identify malicious patterns, monitors for deviations from normal network behaviour and can automatically block or allow traffic based on predefined rules. With an IDS setup, a system should always be safe against malicious

network attacks that aim to affect its availability.

Equally important are identity and access control mechanisms. Authentication is the process of verifying the identity of a user, device, or other entity in a computer system, typically as a prerequisite to granting access to resources in that system. It is the mechanism that confirms whether an entity is who it claims to be. This process often involves validating credentials such as usernames, passwords, digital certificates, or biometric data against an authoritative source that can attest to their integrity and correctness. Multi-factor authentication (MFA) enhances security by requiring two or more pieces of evidence (or factors) to verify the entity's identity, thereby reducing the probability of unauthorised access.

In networked environments, protocols such as the Extensible Authentication Protocol, EAP, illustrated in Figure 2.8, is a framework widely used for the authentication of network clients. It facilitates the exchange of messages during the authentication process between a client (peer) and a server (authenticator). EAP handles requests for identity and credentials, such as One-Time Passwords (OTP) or certificates, and communicates the outcome, whether successful or unsuccessful. While EAP outlines the message exchanges, it doesn't specify the methods for verifying identity. This verification is typically handled by backend protocols like RADIUS or LDAP, allowing EAP to support various network types, including remote access, LAN, and wireless. Although older methods like EAP-MD5 exist, they are no longer considered secure and have been largely replaced by stronger alternatives such as EAP-TLS or EAP-PEAP.

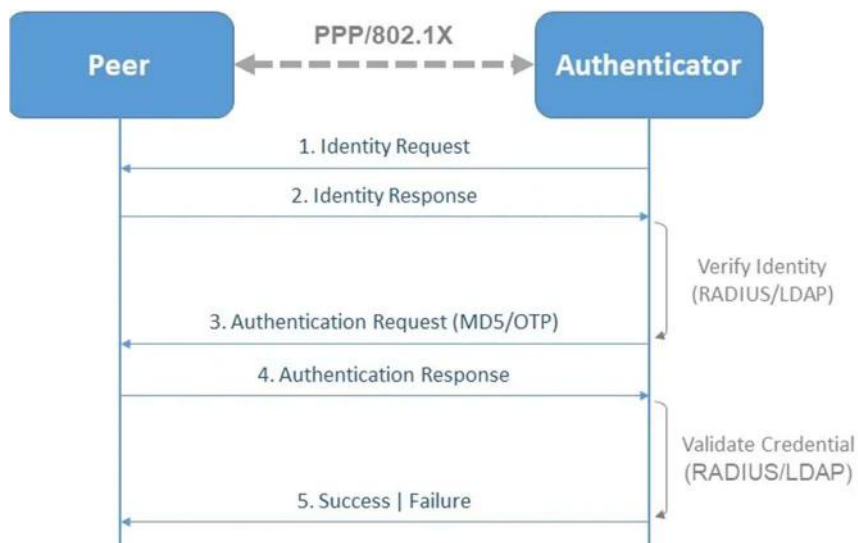


Figure 2.8 – Extensible Authentication Protocol (extracted from [27]).

Authorisation, on the other hand, occurs after authentication and is the process of determining whether an authenticated entity is permitted to perform certain operations or access specific data within a system. Authorisation is inherently tied to the principle of least privilege, which dictates that entities should only be granted permissions necessary to complete their tasks. This limits potential damage from accidents or attacks. Authorisation is managed through settings that are enforced by policies and rules, which can be dictated by roles (role-based access control - RBAC), attributes (attribute-based access control - ABAC), or other factors.

2.2.2 Threat and Risk Modelling

With the increasing number of data breaches and cyberattacks in today's digital age highlights the importance of a proactive security approach. Threat modelling and penetration testing are two such approaches. Threat modelling involves systematically identifying and rating the threats that a system might face. It is a proactive approach to security, helping organisations understand their attack surface, anticipate potential threats, and prioritise security efforts accordingly [28]. In the context of railway systems, threat modelling would involve assessing various components of the 5G network and identifying potential vulnerabilities that could be exploited by attackers. Penetration testing is the practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit [29]. In the railway communication system, penetration testing would involve simulating cyberattacks on the 5G network to identify weaknesses. This hands-on approach complements threat modelling by not just predicting potential vulnerabilities but actively seeking them out in a controlled environment.

One effective framework for threat modelling is the STRIDE model [30] [31] which categorises threats into six types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

- Spoofing is a deceptive technique where a cyber attacker disguises their identity or the origin of their communication to trick the recipient into believing it is legitimate. This can take various forms, such as email spoofing, IP address spoofing, or website spoofing.
- Tampering is a type of cyber threat where an unauthorised party modifies data or system components with the intent to disrupt normal operations, gain unauthorised access, or deceive users. This form of attack can occur at various levels, including data tampering, code tampering, or hardware tampering.
- Repudiation occurs when an individual or entity denies their involvement in a particular transaction or activity.
- Information disclosure involves the unauthorised exposure or release of sensitive information. It can result from security vulnerabilities, inadequate access controls, or malicious actions, potentially leading to privacy breaches.
- Denial of Service is an attack that aims to make a system, service, or network unavailable to users by overwhelming it with excessive traffic or disrupting its normal functioning.
- Elevation of Privilege involves unauthorised escalation of user privileges, granting an attacker higher level of access or control than intended.

Furthermore, the DREAD model can be employed to quantify and prioritise the risks identified during threat modelling and penetration testing. DREAD stands for Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability.

- Damage Potential evaluates the potential harm a successful exploit could cause. The higher the potential damage, the more critical the vulnerability.
- Reproducibility assesses how easily a threat can be replicated by an attacker. If a vulnerability can be exploited consistently with minimal effort or skill, it is deemed to have high

reproducibility.

- Exploitability measures the ease with which a vulnerability can be exploited. It considers the level of technical skill and resources required to exploit it.
- Affected Users estimates the number of users or systems that would be impacted by an exploit.
- Discoverability refers to how likely it is that the vulnerability will be discovered and exploited. It considers factors like the visibility of the system, the complexity of the vulnerability, and whether it is likely to be identified by potential attackers.

By assessing each threat against these criteria, security professionals can better understand the severity of different vulnerabilities and focus their efforts where they are most needed.

2.2.3 Security in Communications

As we transition to 5G networks in railway communications, it is critical to understand the security measures that will keep these systems safe. This section will explore key components such as firewalls, Virtual Private Networks (VPNs), Internet Protocol Security (IPSec), and Transport Layer Security (TLS). Using the simple network diagram in Figure 2.9 as a reference, a breakdown of how each of these elements contributes to the overall security of communications is made.

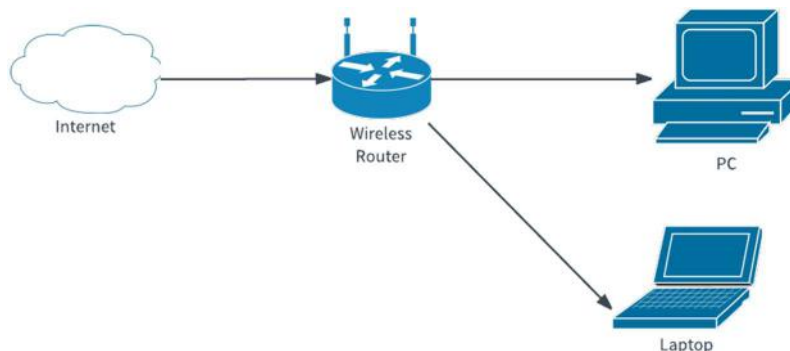


Figure 2.9 – Simplified network diagram.

Firewalls are network security devices designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules [32]. They act as a barrier between a secure internal network and untrusted external networks, such as the internet. They are instrumental in segmenting railway networks into zones, restricting unauthorised access. In this setup, the firewall could be integrated into the wireless router, which is the entry point of the network from the internet. The firewall can examine incoming data packets from the internet, comparing them against its set of rules. If a packet is deemed dangerous or unwanted, like a request from a known malicious source, the firewall can block it from entering the network, thus protecting the PC and laptop from potential attacks. Similarly, the firewall can control the data leaving the network to the internet. This can prevent malicious software on the PC or laptop from sending sensitive data out to the internet. Firewalls can also close ports that are not in use. Ports are virtual data connection points, and open ports can be exploited by hackers. By keeping unnecessary ports closed, a firewall reduces the number of entry points available to malicious users. By setting network access policies, the firewall can restrict access to the network to only

authorised users or systems, reducing the risk of intruders gaining access to the network resources.

In this scenario, a VPN could provide several benefits. A VPN creates a secure and encrypted connection between the PC or laptop and the internet [33]. This encryption protects the data as it travels through the router to the outside network, ensuring that sensitive information remains confidential and safe from eavesdroppers or interceptors. If the laptop is being used at a remote location, such as a coffee shop or an airport, a VPN would allow for a secure connection back to the home network. This would enable the user to access files on the PC or perform tasks as if they were locally connected to the home network, all while maintaining a secure link. Also, a VPN can mask the IP addresses of the devices, making their internet activity more anonymous. This is useful for protecting privacy as it prevents websites and online services from tracking the devices' actual IP addresses and location.

IPSec is a robust suite of protocols designed to secure Internet communications by authenticating and encrypting each IP packet during a session [34]. The primary goal of IPSec is to protect data exchanges over IP networks through cryptographic security services. If the PC or the laptop in the network setup is transmitting sensitive information to a server on the Internet, IPSec can be applied to ensure that this sensitive data is encrypted before it leaves the device. This encryption wraps the data in a secure envelope, making it indecipherable to unauthorised entities who might intercept the transmission. When IPSec is deployed in Transport Mode, it encrypts only the payload of the packet along with the ESP trailer, leaving the original IP header untouched as shown in Figure 2.10. This mode is particularly useful for end-to-end communication, such as a direct connection between the laptop and a secure server on the Internet, ensuring that the message contents remain confidential and unchanged from sender to receiver. Encapsulating Security Payload (ESP) is a component of the IPsec suite used to provide confidentiality (through encryption of the payload), data origin authentication, integrity, and optional anti-replay protection for IP packets. ESP works by encapsulating the original data packet within an ESP header and trailer, encrypting the packet's payload.

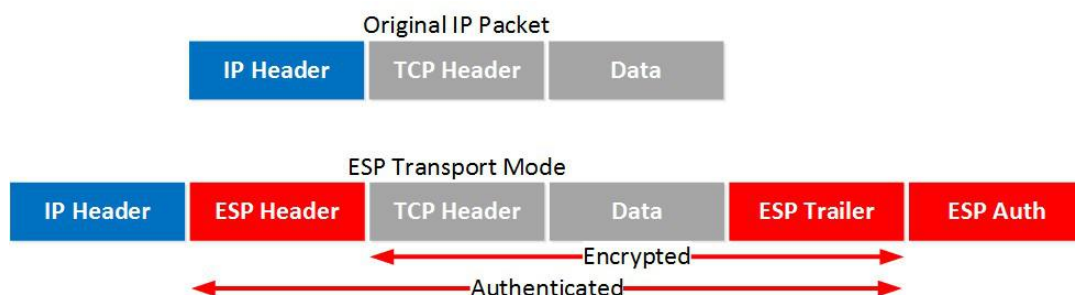


Figure 2.10 – ESP in transport mode.

Alternatively, in Tunnel Mode, IPSec encrypts both the payload and the original IP header, adding a new header to the packet. This approach is frequently adopted in situations where entire networks are connected over the Internet, such as a branch office connecting to the main company network. The router, in this case, would establish a VPN tunnel to another router or gateway, using IPSec to ensure that all data passing through the public Internet is shielded. IPSec guarantees the confidentiality of data so that sensitive information sent from the PC or laptop remains private. It also safeguards the integrity

of the data, providing assurances that the information has not been altered during transit. The authentication feature of IPSec verifies the sender's identity, which prevents data from being spoofed. Lastly, it includes mechanisms for replay protection, which protect against the risk of an attacker capturing legitimate data packets and resending them, potentially creating confusion or unauthorised system access.

Transport Layer Security (TLS) is a cryptographic protocol designed to provide secure communication over a computer network [35]. It is the successor to Secure Sockets Layer (SSL) and is widely used on the internet for securing a variety of communications. In the context of this network diagram with a PC and a laptop connecting to the internet through a wireless router, TLS operates at a different layer of the network stack compared to IPSec. While IPSec operates at the network layer, securing everything at the IP level, TLS operates at the transport layer, which means it is typically used to secure end-to-end communications at the start of the transport layer, securing TCP connections. TLS comes into play once the PC or laptop initiates a secure connection with a server on the internet, like when accessing a website, logging into your email, or purchasing something online. When you visit a website with "https://" in the URL, the browser is using TLS to encrypt the data that will be transmitted between the device and the web server. This encryption ensures that any sensitive information, like passwords or credit card numbers, is not accessible to eavesdroppers who may be intercepting the data as it travels across the network. Part of the TLS handshake process involves the server presenting a digital certificate to prove its identity to the client (the PC or laptop). This helps in ensuring that the user is connecting to a legitimate server and not an impostor.

2.3 Security in 5G

This section outlines an overview of security in 5G networks, detailing the security architecture, authentication mechanisms, privacy issues and known attacks along with their countermeasures.

2.3.1 Security Architecture

Figure 2.11 delineates the comprehensive security architecture within the 5G ecosystem, outlining the integral network functions (NFs) engaged in various authentication-related security protocols. Central to this setup is the User Equipment (UE), which encompasses both the Mobile Equipment (ME) and the Universal Subscriber Identity Module (USIM), the latter being the repository for credentials shared securely with the mobile operator.

Connectivity between the UE and the network's core is managed by the Access and Mobility Management Function (AMF) which operates over the Non-Access Stratum (NAS) protocol. Within this framework, the AMF houses the Security Anchor Function (SEAF), which is integral for primary authentication in conjunction with the Authentication Server Function (AUSF). In addition, the Unified Data Management (UDM) system stores subscription information within the Unified Data Repository

(UDR) and provides additional capabilities, including the Subscription Identifier De-Concealing Function (SIDF) and the Authentication credential Repository and Processing Function (ARPF).

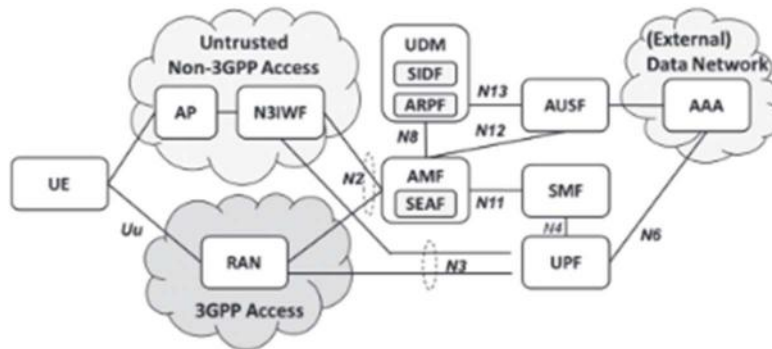


Figure 2.11 – Security architecture (extracted from [36]).

2.3.2 Authentication

Within the 5G framework, numerous features have been enhanced to fortify the mobile system's security and resilience, surpassing the capabilities of its predecessors. A key highlight is the revamped authentication mechanism, which now includes two primary methods: the 5G Authentication and Key Agreement (5G AKA) and the Extensible Authentication Protocol AKA' (EAP-AKA') [36]. There are four types of authentications: primary and secondary authentication, slice authentication and authentication for massive Internet of Things applications.

Primary authentication establishes a two-way verification between the UE and the network provided by the operator. Through the AKA process, the serving network validates the Subscription Permanent Identifier (SUPI) of the UE, and reciprocally, the UE authenticates the serving network's identifier using an underlying key authentication mechanism. This method ensures that both parties are authenticated by the successful application of keys that are generated during the AKA, which are then used to secure messages in both the control and user planes. The other three types of authentications are not relevant to the railway scenario so they will not be further explained. More information about them can be found in [36].

The AKA protocol involves a challenge-response mechanism where the network sends a challenge to the user's device. The device responds with a proof of identity, encrypted with a secret key shared with the network. This ensures that only legitimate users can access the network, while simultaneously establishing encryption keys for securing subsequent communications. Although this protocol is considered secure, the analysis done in [37], shows that there are some shortcomings with this protocol, such that the location privacy of the UE can be compromised; there is no perfect forward secrecy, which ensures session keys are not compromised even if the long-term secret keys are breached, in the case of some keys being leaked; and that the serving network could be vulnerable to DoS attacks.

2.3.3 Privacy

In 5G systems, the Subscription Permanent Identifier (SUPI) is a sensitive piece of information that includes the subscriber's unique identity and subscription details [38]. As illustrated in Figure 2.12, the system is designed to protect this identifier from exposure, especially when transmitted over the air. To ensure subscriber privacy, the SUPI is never sent in plaintext form over the network. Instead, the UE generates a Subscription Concealed Identifier (SUCI), which conceals the sensitive parts of the SUPI using cryptographic protection.

The process begins at the UE, where the SUPI is composed of three components: the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscription Identification Number (MSIN), which is the most privacy-sensitive part. The MCC and MNC are retained in plaintext for routing purposes, while the MSIN is encrypted using an asymmetric encryption algorithm. Specifically, the UE uses the Home Network's public key and a refreshing parameter to encrypt the MSIN through an Elliptic Curve Integrated Encryption Scheme (ECIES). This results in the SUCI, which contains the MCC, MNC, and the encrypted MSIN, along with metadata identifying the encryption scheme and the key used. This mechanism ensures that the identity of the subscriber remains protected, even if the SUCI is intercepted.

Once the SUCI reaches the subscriber's home network, it is processed by the Subscription Identifier De-Concealing Function (SIDF), which is located within the Authentication credential Repository and Processing Function (ARPF) or Unified Data Management (UDM). The SIDF uses the corresponding private key, along with the same refreshing parameter, to decrypt the encrypted MSIN. The decryption process also relies on the ECIES algorithm. After decryption, the MSIN is reconstructed and combined with the MCC and MNC to recover the original SUPI. This allows the home network to securely and privately identify the subscriber without having exposed the SUPI during transmission.

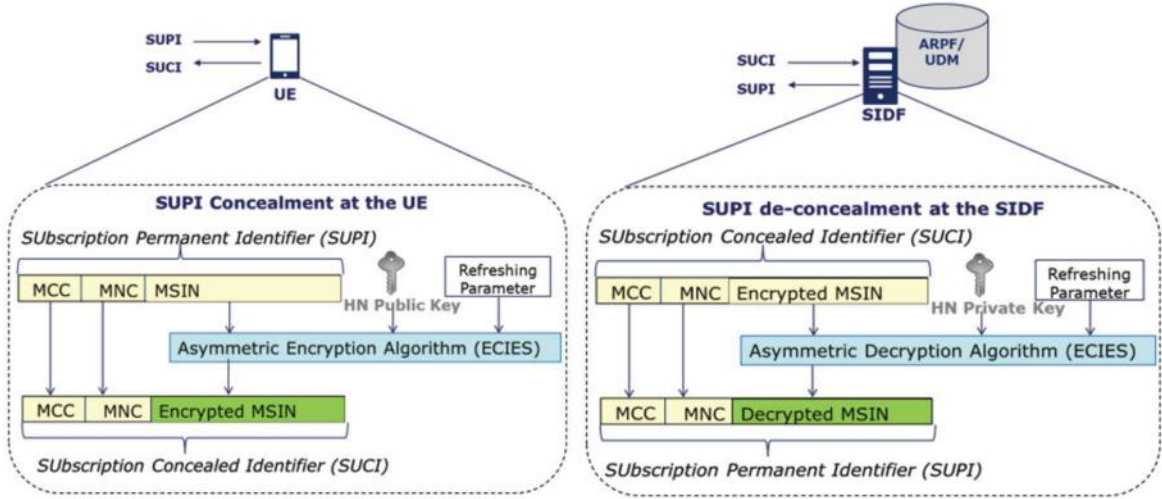


Figure 2.12 – SUPI structure and concealed sensitive information (extracted from [38]).

2.3.4 Attacks and Countermeasures

Security threats targeting networks can be categorised into four primary types: insider, outsider, network,

and virus attacks. Insider attackers disrupt control and execution functions from within the organisation. Outsider attackers, on the other hand, aim to interfere with the communication system either by data monitoring or by accessing confidential information. Network attackers focus on destabilising the network's operation or completely shutting it down. The virus category encompasses threats like malware, worms, and other software-based attacks designed to infiltrate systems for harmful purposes.

These threats can also be divided based on their targets: user-directed attacks and network-directed attacks. User-directed attacks include device triggers, which involve impersonating the network to send unnecessary commands to machines, leading to energy depletion; node capture, where attackers gain complete control over a device by exploiting its physical vulnerability; and privacy leaks due to data integrity flaws.

Network-directed attacks encompass congestion control manipulation, which affects the network's ability to manage traffic efficiently; piggybacking, where harmful data is hidden within legitimate data transfers; and signalling attacks, characterised by repeated unauthorised access requests that overload the system.

The following Figure 2.13 illustrates a selection of potential security attacks that could target 5G networks, showcasing various methods attackers might use to breach the network's defences.

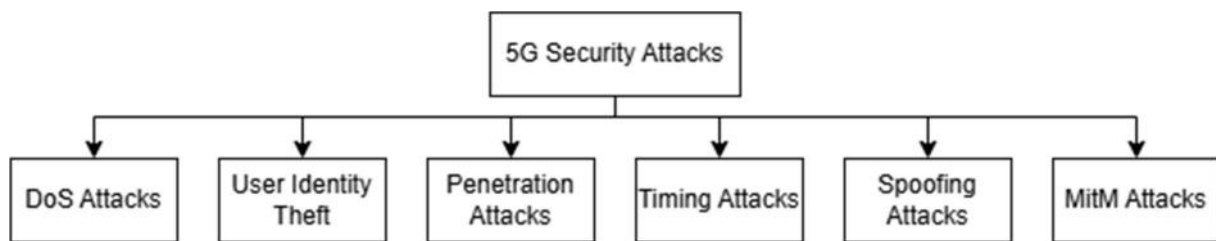


Figure 2.13 – Example of some attacks against a 5G network (adapted from [39]).

It is important to note that while these represent some of the key vulnerabilities, the full spectrum of threats against 5G infrastructure is even broader, with numerous other tactics and exploits that security professionals must guard against to ensure robust network protection [39].

- DoS and Jamming Attacks: These involve overwhelming the network with unnecessary traffic or signals to prevent legitimate use, with jamming specifically targeting communication channels with noise or false signals.
- Eavesdropping: Unauthorised interception of data, either passively (simply listening in) or actively (sending signals to interfere with users).
- Pilot Spoofing and Masquerade Attacks: The former sees attackers mimic legitimate users, while the latter involves assuming fake identities to gain unauthorised access to data and devices.
- Sybil and DoD Attacks: Sybil attacks involve the creation of multiple false identities to overwhelm the network, and DoD (Denial of Defence) attacks aim to prevent network problem detection.
- Injection and Replay Attacks: Injection attacks involve the insertion of fake messages into the system, whereas replay attacks disturb system functioning by resending captured legitimate

messages.

- **Spoofing and Collision Attacks:** Spoofing involves sending incorrect information, such as messages or headers, to mislead systems or induce collisions in network responses.
- **Synchronisation Disruption and Network Access Attacks:** These disrupt network timing or allow unauthorised access to network infrastructure, leading to potential control over the system.
- **Traffic Attacks:** This encompasses both confidentiality attacks, which compromise the privacy of network traffic, and integrity attacks, which alter traffic to disrupt its original intention.
- **Man-in-the-Middle and Malware Attacks:** These redirect or manipulate traffic, with malware installing harmful software on devices without user knowledge.
- **Illusion and Bogus Information Attacks:** These create fake events or send false information to deceive users into making incorrect decisions.
- **Timing, Impersonation, and Hijacking Attacks:** Timing attacks introduce delays in communication, impersonation attacks use fake identities, and hijacking takes over communications or devices for malicious ends.
- **Evil-Twin Attacks:** These involve setting up unauthorised access points that mimic legitimate ones to trick users into connecting, thus compromising their privacy.

Understanding the various types of attacks that can target 5G networks is crucial in developing robust defences. It is not just about recognising the threats but also about countering them effectively. Some of the most prevalent attacks, such as DoS, eavesdropping, and spoofing, have well-researched countermeasures that can greatly enhance network security. For example, to combat DoS attacks, which flood networks with excessive traffic, techniques like rate limiting and traffic filtering can be employed. Against eavesdropping, encryption remains one of the most powerful tools, ensuring that intercepted communications cannot be easily deciphered [40]. Spoofing attacks, where attackers disguise malicious communications as legitimate, can be countered with authentication protocols that confirm the identity of each communication endpoint. With these examples in mind, for every type of attack, there can be a suite of countermeasures tailored to prevent, mitigate, or eliminate the threat. To better illustrate this, a summarised table that pairs some of the prominent attack types with their potential countermeasures is shown below.

Table 2.1 only shows various types of attacks, and their respective countermeasures, that can target a 5G network, each posing different threats such as compromising confidentiality, integrity, and availability. Notably, some countermeasures like authentication and encryption are versatile, providing defence against multiple attack vectors. This means that instead of looking for a single countermeasure for a single attack, it is possible to counter various attacks with a single measure.

Table 2.1 – Some attacks and their countermeasures (adapted from [39]).

Attack	Target	Countermeasure
Eavesdropping	<ul style="list-style-type: none"> Confidentiality 	<ul style="list-style-type: none"> Authentication Encryption
DoS Attack	<ul style="list-style-type: none"> Integrity Availability 	<ul style="list-style-type: none"> IDS Authentication Firewalls
Tampering	<ul style="list-style-type: none"> Confidentiality Integrity Authentication 	<ul style="list-style-type: none"> Database encryption Authentication Restricted access to hardware
Man-in-the-middle	<ul style="list-style-type: none"> Confidentiality Integrity 	<ul style="list-style-type: none"> Authentication Data encryption before transmission

2.4 Services and Applications

This section discusses 5G services and applications, focusing on how this technology enhances communication capabilities and supports a wide range of applications. It details the improved speed, reliability, and network capacity of 5G, which enable advanced services like high-speed mobile broadband, massive machine-type communications, and ultra-reliable low-latency communications,

Modern mobile networks support a variety of services, essentially categorised into audio, video, and data [41]. These categories are fundamental to the applications used daily, from calling and streaming to browsing and downloading.

Quality of Service (QoS) and Quality of Experience (QoE) are two critical metrics used to ensure these services meet user needs. QoS focuses on network performance, like speed and reliability, while QoE measures user satisfaction with these services.

It is highlighted that services are organised into four distinct classes based on their operational characteristics and requirements:

- The Conversational class includes real-time services like voice and video calls, requiring low latency for seamless communication. Symmetry in data rates is essential to support the bidirectional nature of these services.
- Streaming services, encompassing video and music streaming, demand real-time delivery but with a tolerance for slight variations in delay. The data flow is predominantly unidirectional, reducing the need for symmetric data rates.
- The Interactive class covers services such as web browsing and online gaming, where timely

interaction is crucial but not necessarily in real-time. These services can accommodate moderate delays and do not necessitate symmetric data flow.

- Lastly, Background services operate without immediate user interaction and include activities like email synchronisation and software updates. These services are characterised by their tolerance for high delays and asymmetric data rates, optimising network resource use without compromising the performance of more delay-sensitive services.

Services are prioritised based on their requirements and importance. For example, voice and video calls need low latency and are given higher priority to ensure clear, uninterrupted communication. On the other hand, services like email, which don't require real-time interaction, can handle higher latency and lower priority.

LTE and upcoming technologies like NR introduce classifications like Guaranteed Bit Rate (GBR) and non-GBR, plus Quality Channel Indicators (QCI), to manage and allocate network resources effectively. These classifications help the network differentiate service needs, ensuring that critical services get the necessary resources without impacting less critical ones.

Regarding application characteristics, they are defined by their need for speed (bit rate) and responsiveness (latency). Real-time applications, such as gaming or live streaming, demand high bit rates and low latency. Non-real-time applications, like web browsing, can operate with lower bit rates and higher latency without significantly affecting the user experience.

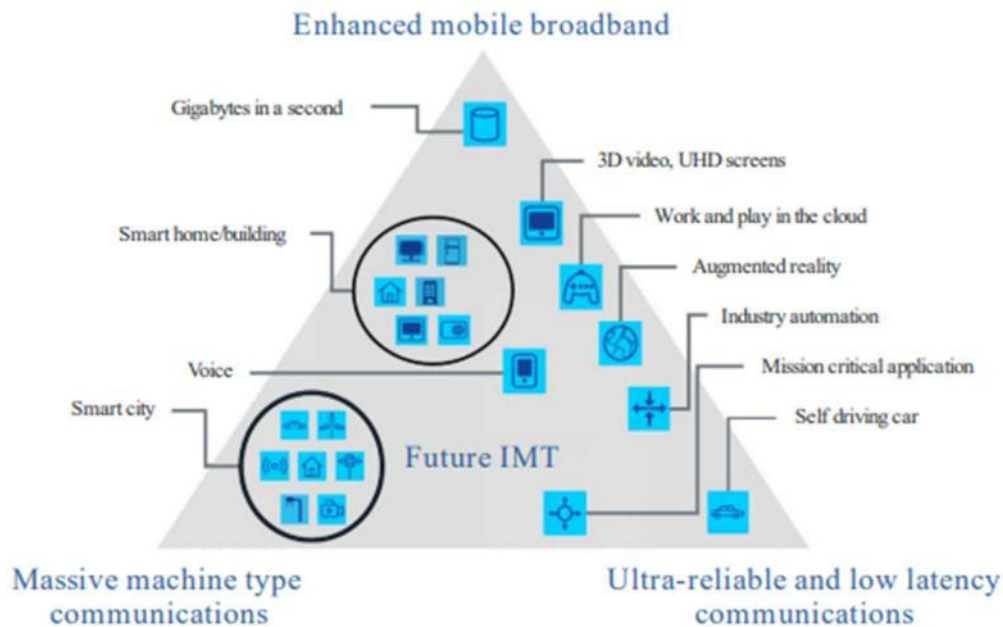


Figure 2.14 – 5G key features (extracted from [42]).

As mentioned in [42], the 5G system is supposed to support various new use cases, Figure 2.14, which can be classified into three features:

- Enhanced Mobile Broadband Connectivity (eMBB): This type of use case is like current ones but represent the growing scenarios of a fully connected society. New services like augmented reality and three-dimensional service will play a more important role in the 5G timeframe.

Moreover, the demand for mobile communications in vehicles, high-speed trains and even aircraft is growing.

- Massive Machine Type Communications (mMTC): This family includes both low-cost, low-power, long range MTC and broadband MTC. Soon, ultra-light, low power sensors may be integrated into people's clothing to measure various environmental and health attributes. Smart services will be pervasive in urban and rural areas for metering, environment monitoring and traffic control. These services result in very high device density.
- Ultra-Reliable Critical Communication Services (URCC): This category covers use cases with strong demand on real-time interaction.

2.5 Railway Communications

This section examines the network architecture and the services and applications vital for railway communications. It outlines the specific network components including control centres, base stations, and train stations, and their interconnected roles in facilitating railway operations. Additionally, the section explores various communication services utilised in railways, such as voice communications, control and signalling information, and data services. At the end of the section is a brief subsection where issues with security in railways are discussed.

2.5.1 Railway Network

The designed railway infrastructure can be illustrated by the general architecture shown in the following Figure 2.15, and is composed of:

- Control Centre (CC): This is the central hub that manages and controls the overall railway network. It monitors and directs the traffic of trains, ensures the safety and scheduling, and handles any emergencies that arise. The control centre is connected to both base stations and train stations through optical fibres, ensuring a stable and high-speed connection.
- Base Station (BS): These are fixed points along the railway tracks that serve as communication hubs between the moving trains and the control centre. Base stations are interconnected, likely for redundancy and to hand off communication with trains seamlessly as they move. They are also connected directly to train stations through optical fibre.
- Train Station (TS): These are the stations where passengers board and disembark from trains. They are not a subject of this study and are only represented for reality purposes.

The connections between these entities are made through optical fibres and radio frequency. Optical fibre is the medium through which high-speed data communication occurs between the control centre, base stations, and train stations. They provide a reliable and fast method for transmitting large amounts of data over long distances without significant loss. 5G radio frequencies enable data transmission between the trains and base stations. This allows for continuous monitoring and control of trains.

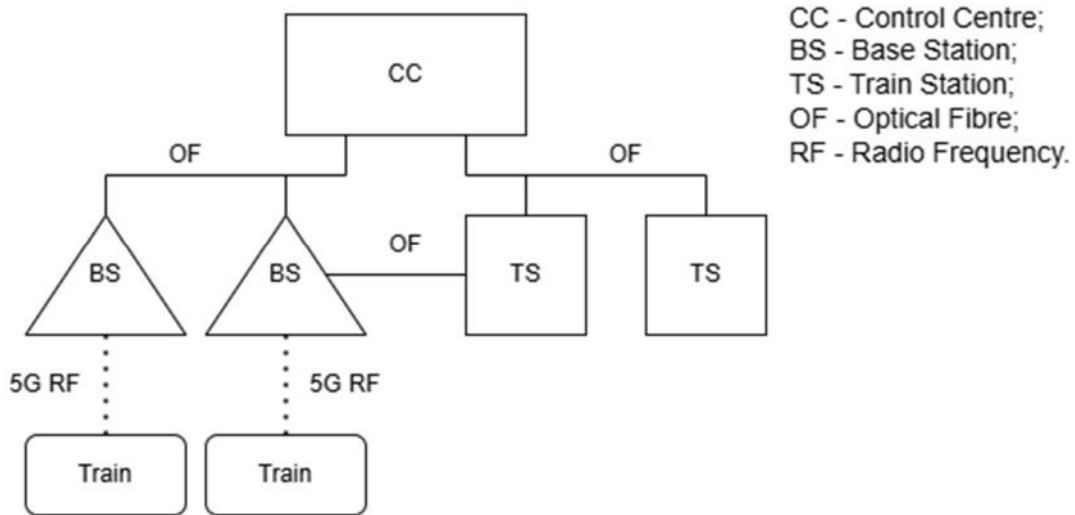


Figure 2.15 – General railway architecture.

2.5.2 Services and Applications

The diverse uses of railway communications can be categorised into four primary types of services: voice communications, non-safety critical information, control and signalling information, and video along with other high-capacity services.

Voice services in railway communications are divided into five types of sub-services[43]: direct calls between two parties, calls for public emergencies, calls broadcast to a wide audience, calls within a group, and calls involving multiple parties. Public emergency calls enable contact with external services like ambulance services in emergencies, while broadcast and group calls utilise VBS (Voice Broadcast Service) and VGCS (Voice Group Call Service) respectively.



Figure 2.16 – GSM-R voice services (extracted from [44]).

These sub-services, Figure 2.16, are applicable in various operational contexts, including dispatching, shunting, and maintenance. Dispatching involves communication between the train drivers, using the radios in their cabs, and the dispatching staff, who use the fixed terminals in the Control Centres. The purpose is to ensure the correct operation of the train. Shunting refers to the communication between

train drivers and shunting staff to carry out shunting operations. Shunting is the process by which carriages are maneuvered to assemble complete trains or to disassemble them. Maintenance includes communication between the rail track workers, utilising handheld terminals, and the dispatching staff at the Control Centres via fixed terminals. This is essential for coordinating maintenance work on the railway line and related tasks.

The data service in railway communications is segmented into four distinct sub-services [43]. Of these, three are designated as non-safety-critical data services: text messaging, general data applications, and automatic fax transmission. The fourth sub-service pertains to applications related to train control and signalling. This category is deemed as safety-critical data due to its importance in operational security. ERTMS stands as the system tasked with overseeing control and signalling responsibilities, encompassing two primary components: ETCS for control and signalling, and GSM-R for the requisite data transmission. The ETCS is further broken down into four key operational levels, ranging from Level 0 to Level 3. A brief overview of each level was already provided in Section 2.1.1.

Finally, broadband services are geared towards providing applications that cater to both infotainment needs and the security of passengers, such as:

- High-definition Television (HDTV): This service includes onboard television for infotainment applications.
- Closed-circuit Television (CCTV): It provides a live video stream and recording capabilities of onboard cameras.
- Public address: This service is responsible for announcements made through an advanced IP system.
- Platform cameras: They offer a live video stream from station platform cameras directly to the driver's cab.
- Passenger information: This service entails multimedia messages that are displayed on monitors within the cab and on platform monitors.
- Help points: These are infotainment devices designed for passenger interaction.
- Equipment management: It involves real-time monitoring of onboard equipment.
- High-speed internet access: This service provides passengers with access to high-speed internet.

Also, 3GPP outlines specific performance criteria for various applications in railway contexts for mainlines, detailed below in Table 2.2. The table provides a structured comparison of the communication requirements for three major categories of railway services, Safety-related applications, Mission-critical services, and non-critical services, across several key performance indicators. These indicators include latency, reliability, mobility and throughput, among others. The aim of this table is to illustrate the diverse and sometimes conflicting requirements that railway communication systems must support. Safety-related applications, such as train control signalling, demand ultra-low latency and very high availability to ensure passenger safety and system reliability. In contrast, non-critical services like passenger internet access or entertainment tolerate higher delays and lower availability.

Table 2.2 – Performance requirements for railway scenarios (adapted from [45]).

Scenario	End-to-end latency [ms]	Reliability [%]	Speed limit [km/h]	User experienced data rate	Payload size (Note 1)	Area traffic density	Service area density (Note 2)
Voice Communication for operational purposes	≤100	99.9	≤500	100 kbps up to 300 kbps	Small	Up to 1 Mbps/line km	200 km along rail tracks
Critical Video Communication for observation purposes	≤100	99.9	≤500	10 Mbps	Medium	Up to 1 Gbps/km	200 km along rail tracks
Very Critical Video Communication with direct impact on train safety	≤100	99.9	≤500	10 Mbps up to 20 Mbps	Medium	Up to 1 Gbps/km	200 km along rail tracks
	≤10	99.9	≤40	10 Mbps up to 30 Mbps	Medium	Up to 1 Gbps/km	2 km along rail tracks urban or station
Standard Data Communication	≤500	99.9	≤500	1 Mbps up to 10 Mbps	Small to large	Up to 100 Mbps/km	100 km along rail tracks
Critical Data Communication	≤500	99.9999	≤500	10 kbps up to 500 kbps	Small to medium	Up to 10 Mbps/km	100 km along rail tracks
Very Critical Data Communication	≤100	99.9999	≤500	100 kbps up to 1 Mbps	Small to Medium	Up to 10 Mbps/km	200 km along rail tracks
	≤10	99.9999	≤40	100 kbps up to 1 Mbps	Small to Medium	Up to 100 Mbps/km	2 km along rail tracks
Messaging	–	99.9	≤500	100 kbps	Small	Up to 1 Mbps/km	2 km along rail tracks
NOTE 1: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.							
NOTE 2: Estimates of maximum dimensions							

2.5.3 Security in Railway Communications

Railway systems have increasingly faced cyberattacks over the last two decades, affecting operations and safety. The following Table 2.3 lists significant incidents where hackers targeted rail networks, causing disruptions ranging from signal system failures to ransomware attacks on rail infrastructure.

One of the most illustrative incidents that demonstrates the intersection between physical and cyber vulnerabilities in railway infrastructure occurred in January 2008 in Lodz, Poland [2]. A teenager was able to exploit weaknesses in the city's tram control system by constructing a homemade remote control using parts from a television and publicly accessible information about the tram network. By manipulating the track switching mechanisms, he caused the derailment of four tram vehicles, injuring twelve people. This event revealed not only the lack of physical protection around critical components but also the absence of proper authentication mechanisms to restrict access to sensitive control signals. Although the method was relatively unsophisticated, the consequences were significant, emphasising

that even attackers with limited resources and technical expertise can disrupt transport systems when fundamental security controls are lacking.

Table 2.3 - Timeline of cybersecurity incidents in the railway sector (adapted from [46]).

Date	Description
August 2003	A computer virus disabled the CSX Transportation headquarters in Florida, affecting signalling in thousands of km of railway line.
January 2008	A teenager derailed four tram vehicles causing injuries to twelve people after hacking a train network of Lodz, Poland.
December 2012	A cyberattack on a Northwestern US rail company’s computers disrupted railway signals for two days.
March 2015	The HoneyTrain Project recorded over two million login attempts within four successful illegal accesses to the Human-Machine Interface (HMI) of a virtual train control systems in the space of six weeks.
October 2017	Sweden’s transportation Administration was targeted by a DDoS attack on the IT systems that monitor railway traffic. Two DDoS attacks hit the public transportation operator Västtrafik the next day.
May 2018	The Danish operator DSB came under a DDoS attack, making it impossible to purchase tickets. Internal mail and telephone systems used by the DSB staff were also affected.
July 2021	A cyberattack on Iran’s railroad system caused chaos across the whole country.
April 2022	Linked to events in the Russian-Ukrainian conflict, a "clandestine network of railway workers, hackers and dissident security forces went into action to disable or disrupt the railway links connecting Russia to Ukraine through Belarus".

As seen before, some of the most disruptive attacks on railway networks are Denial of Service (DoS) and Jamming attacks.

Denial of Service (DoS) attacks can severely disrupt railway systems, particularly those reliant on automated and cooperative controls like high-speed trains. These attacks block the transmission of crucial operational data between trains and control centres, leading to a loss of control and coordination. This loss of communication can cause significant delays and disruptions in train schedules, impacting service reliability and passenger convenience.

To counteract DoS attacks, railway systems can adopt a resilient control scheme that maintains essential train functions during an attack [47]. This involves implementing detection mechanisms that use an acknowledgment-based strategy where a lack of received acknowledgment indicates a possible DoS attack. Recovery mechanisms are also crucial, enabling quick restoration of communication networks through backup channels or systems. Additionally, enhancing firewall rules to restrict traffic only to known and trusted sources and implementing rate-limiting controls can help prevent flood attacks.

Jamming the connections in a railway network can happen when an attacker uses a device to emit radio frequency signals that interfere with the communication channels [48]. This can be achieved with relatively simple hardware that broadcasts noise, or the same frequency used by the railway's communication systems, effectively drowning out legitimate signals. Such an attack could delay or block the transmission of emergency signals, causing critical communication failures during incidents where swift response is vital. It could also prevent the proper functioning of signalling systems, leading to potential safety hazards like train collisions or derailments due to miscommunication or a lack of communication.

In the event of a jamming incident, railway systems should be designed to immediately switch to alternate frequencies or communication mediums. Pre-established emergency protocols, such as alternative signalling procedures or manual operations, should be activated to maintain control over train movements and ensure passenger safety. Communication with trains and personnel via secondary channels, including satellite phones or other secure lines not affected by the jamming, should be initiated to coordinate manual interventions. Two commonly used anti-jamming strategies are MIMO-Based jamming mitigation and channel hopping [49].

MIMO-Based jamming mitigation employs Multiple Input Multiple Output (MIMO) technology to handle reactive jamming attacks, particularly in Wi-Fi networks. It uses interference mitigation techniques like projecting the received signals into a subspace orthogonal to the jamming signals, allowing the legitimate signal to be decoded using techniques such as zero-forcing. This method is particularly effective as it does not require complete knowledge of the jammer's channel, relying instead on the estimated channel ratios from known pilots or received signals.

Channel hopping improves the reliability of wireless communications by frequently switching the communication channel. It is effective against reactive jamming, where jammers target specific frequencies. In environments like Bluetooth and Wi-Fi, channel hopping can prevent jammers from continuously disrupting the signal, as they must guess or re-detect the channel on which the communication has moved.

2.6 Related Work

This chapter explores the related work that exists about the integration of 5G technology into railway communications. 5G in railways is relatively new, so there aren't many works around it, much less works on the cybersecurity aspect.

5G Railways (5G-R) based on the 5G SA architecture represents a significant technological advancement in rail transport [50], [51]. 5G SA offers higher data rates, lower latency, and more reliable connections compared to GSM-R which translates to more efficient and real-time data processing capabilities, crucial for train control and monitoring systems, which also allows for the potential for autonomous train operations. The enhanced connectivity provided by 5G allows for the implementation

of sophisticated safety and monitoring systems on trains. High-definition cameras, sensors, and other IoT devices can transmit real-time data, enabling quick responses to any safety issues or maintenance requirements. Passenger experience will also be improved since 5G provides high-speed internet, allowing for new services to be provided to passengers, like seamless streaming, gaming, and browsing capabilities during journeys.

As talked about before, 5GRAIL [7] is a project being developed to meet the FRMCS specifications and make the transition from GSM into 5G possible. 5GRAIL aims to reduce specific equipment costs and installation engineering time by combining all train-to-ground communications, with an on-board setup based on standardised interfaces and including mainstream 5G components, called TOBA (Telecom On-Board Architecture). Prototypes have been tested in simulated and real environments, with pilots in labs and in the field that were rolled out in various European sites (France, Hungary and Germany), to ensure compliances and validation for the FRMCS version 1 specifications [52].

The theoretical work done by R. He [53] reviews the current advancements in railway communications and discusses the implementation of 5G technology for intelligent railways. It outlines the potential of 5G in improving service delivery, operational efficiency, and safety by providing high-speed connectivity and support for a variety of advanced applications. The paper also analyses key 5G technologies such as network architecture and massive MIMO, while addressing the challenges in implementing 5G for railway systems. Similarly, A. Gonzalez-Plaza's work [54] highlights the increasing need for high-quality, high-capacity communications for train control and passenger services due to the rapid growth of railway transportation. It discusses the insufficiency of current systems and positions 5G as a necessary advancement to meet these demands. It outlines the key characteristics and requirements for critical and non-critical communications in railways, offering insights into the technologies suitable for near-future implementation in the sector.

Although a bit old and outdated, an article written by Carlson [55], explores the evolving landscape of railway security, particularly in the context of technological advancements. It discusses how modern technologies, including microprocessors and networked systems, are being integrated into railway systems, enhancing operational efficiency and communication capabilities. However, this integration also brings vulnerabilities, making rail systems potential targets for cyberattacks. The paper examines the potential risks and the need for comprehensive security measures, highlighting the importance of both physical and network security in protecting railway infrastructure and operations.

The paper by Mikko Kiviharju [56] addresses the cryptographic and key management aspects crucial for secure railway communications. It also outlines the complexities of ensuring robust cybersecurity in an open railway environment, considering the enhanced risk of cyberattacks with more sophisticated technology. It suggests the need for in-depth security measures beyond traditional approaches to protect against threats and ensure safety in railway operations.

The security aspect of 5G in railway communications is a relatively novel area of study, and consequently, the research specifically addressing this subject is very limited.

2.7 Chapter 2 Summary

Chapter 2 presents the background necessary to understand the integration of 5G technology into railway communication systems, focusing on core concepts of mobile communications, cybersecurity, services and applications, and the current state of railway networks.

Section 2.1 introduces the evolution of mobile communication technologies, beginning with GSM and its railway-specific extension, GSM-R, which has been the standard for railway communications in Europe. It then transitions to 5G, highlighting its advantages over previous generations, particularly in terms of higher bandwidth, lower latency, and increased device connectivity. These improvements are essential for enabling advanced railway services, such as autonomous train control, real-time monitoring, and high-speed data transmission.

Section 2.2 explores key cybersecurity principles, starting with foundational concepts like confidentiality, integrity, availability, and authentication. A specific focus is placed on threat and risk modelling, where frameworks like STRIDE and DREAD are introduced to help identify, classify, and prioritise potential security vulnerabilities.

Section 2.3 focuses on the security mechanisms embedded in 5G networks. It explains how 5G introduces improvements over previous generations through features like mutual authentication, better encryption, and integrity protection of user and signalling data. The section describes how 5G's layered architecture allows for enhanced security in different parts of the network and addresses how it handles identity protection.

Section 2.4 discusses the services and applications supported by 5G. It classifies services into conversational, streaming, interactive, and background types based on their latency and bandwidth needs. The section also highlights Quality of Service (QoS) and Quality of Experience (QoE) as key performance indicators for ensuring user satisfaction. Furthermore, it introduces the three major use case categories of 5G: Enhanced Mobile Broadband (eMBB), Massive Machine-Type Communications (mMTC), and Ultra-Reliable Low-Latency Communications (URLLC).

Section 2.5 focuses specifically on railway communications. It details the architecture of a typical railway network, which includes control centres, base stations, and train stations connected via optical fibre and 5G radio links. It describes the communication services used in railways, such as voice communication, control and signalling systems, and data services. Each service type plays a crucial role in operations like dispatching, maintenance, and safety. The section also presents 3GPP-defined performance requirements for various railway scenarios, covering parameters such as latency, reliability, and throughput.

Section 2.6 reviews related work on 5G integration in railway systems. While 5G in this context is still a developing area, several initiatives, such as the 5GRAIL project, are already working toward meeting the FRMCS standards and replacing GSM-R. The section highlights studies that explore the advantages of 5G for operational efficiency, safety, and passenger experience.

Chapter 3

Railway Architecture

Chapter 3 describes the architecture of railway communication networks. It covers the main components, including railway services, the general system architecture, and specific architectures for the control centre, train, and base station. This chapter provides the technical foundation needed to understand the network structure before analysing security risks in the next chapter.

3.1 Railway Services

Railway services can be divided into two broad categories: Operational and Passenger services. These services are further classified into Critical and Non-Critical based on their importance to the overall functioning and safety of the railway system. These services and their categorisations can be seen in the following Figure 3.1.

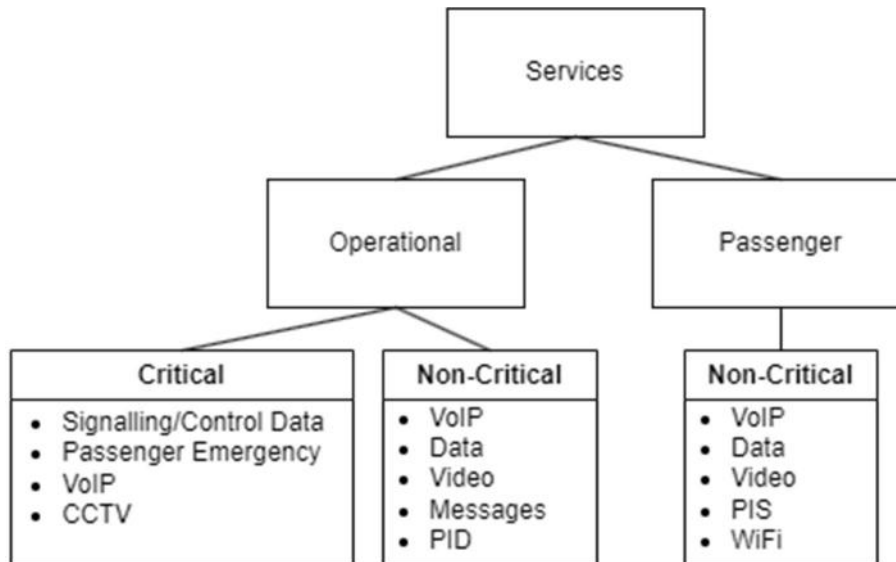


Figure 3.1 – Railway services.

Operational services directly impact the railway's infrastructure and its ability to run smoothly. They are split into Critical and Non-Critical services. Critical operational services are the backbone of railway safety and efficiency. They ensure that essential functions such as signalling, train control, and emergency communication systems operate without disruption. These services are integral to avoiding accidents, maintaining schedules, and ensuring real-time coordination between trains and control centres.

- Signalling and control data systems are among the most critical services in any railway network. These systems are responsible for controlling train movements, managing speed, and ensuring safe distances between trains. The data transmitted through these systems directly affects the coordination between trains and railway control centres, ensuring that trains operate safely and on schedule.
- Passenger emergency systems, such as emergency switches located inside trains, allow passengers to alert train personnel in case of an emergency. These switches enable passengers to trigger immediate actions, such as stopping the train or alerting authorities in cases of accidents, fires, or other critical incidents.
- VoIP services allow train drivers and personnel to make emergency calls to railway control centres or other authorities during critical situations. These calls are essential for real-time communication during incidents such as system malfunctions, accidents, or medical emergencies on board.

- CCTV systems provide real-time video surveillance of the train and its surroundings, enhancing both operational security and passenger safety. CCTV footage is critical in monitoring security incidents, such as vandalism, theft, or potential terrorist activities. It also plays a vital role in post-incident investigations.

Passenger services, which are classified as non-critical, focus on enhancing the passenger experience, such as WiFi connectivity and entertainment services. Although important for customer satisfaction, interruptions in these services do not pose immediate safety risks and will not require further study.

Table 3.1 – Critical service requirements and specifications.

	Signalling/Control	Pass. Emergency	VoIP	CCTV
Data Rate per Terminal [Mbps]	0.1	0.1	0.1	2
Number of Terminals	1	1	2	12
Data Rate per Train [Mbps]	0.1	0.1	0.2	24
Priority	1	2	3	4
Reliability [%]	99.9999	99.999	99.99	99.9
Availability [%]	99.9999	99.999	99.99	99.9
Latency [ms]	≤5	≤5	≤5	≤10
Packet Loss Ratio [%]	10 ⁻⁶	10 ⁻⁶	10 ⁻⁶	10 ⁻³

In Table 3.1, four critical railway services are analysed, arranged from the highest priority on the left to the lowest priority on the right. For each service, the table presents key performance metrics: data rate per terminal, the number of terminals, and data rate per train (which is the product of the first two, representing the total data rate required per train). The table also outlines other essential parameters such as latency, reliability, and availability, highlighting the operational demands of each service. The parameters presented illustrate the differing needs of these critical services, with higher-priority services like signalling/control and passenger emergency requiring stricter performance thresholds compared to VoIP and CCTV systems, which have lower priority but still play essential roles in the railway's safety and operation.

3.2 General Railway Architecture

The high-level architecture of the railway communication system is shown in the following Figure 3.2. It consists of several key components and their connections:

- CC (Control Centre): This is the central hub responsible for managing and overseeing the entire railway network. It receives and processes data from various subsystems and makes critical decisions regarding train operations. The CC is connected to the BSs and the TSs through optical fibre. For this thesis, both the optical fibre connections and CC itself are not considered and as entry point for the attacker, meaning that an attacker cannot directly access and

compromise these components. This does not mean they are secure, since if an attacker gains access to the BS or the Train, the CC could still become compromised.

- BS (Base Station): The base station facilitates communication between the control centre and trains. It acts as an intermediary, enabling data transmission and reception, such as signalling, control data, and other information. This component is considered vulnerable, since an attacker can compromise it through physical and radio means.
- TS (Train Station): The train station facilitates communication and coordination when trains arrive, depart, or stop. It supports interactions between the train and control centre, ensuring proper scheduling, passenger handling, and safety during train operations at the station. However, the TS will not be analysed in this thesis, as it essentially functions like a base station and primarily provides non-critical services to passengers. It is included here only for completeness and to reflect the real-world architecture.
- TRAIN: This represents the train itself, equipped with a Mobile Terminal (MT). This MT is composed of an antenna located on top of the train, and its computing components, inside the train itself. The train communicates with both the base station and control centre, transmitting operational data, emergency alerts and receiving control signals. Like the BS, this component is also vulnerable to physical and radio attacks.
- CR (Control Room): Located within the train, inside the driver's cabin, the control room is where onboard staff monitor train operations and interact with the communication network. It is responsible for responding to instructions from the control centre or addressing any onboard emergencies. Although this component is in a secure location, an attacker can force its entry inside it, so it is deemed as physically vulnerable.

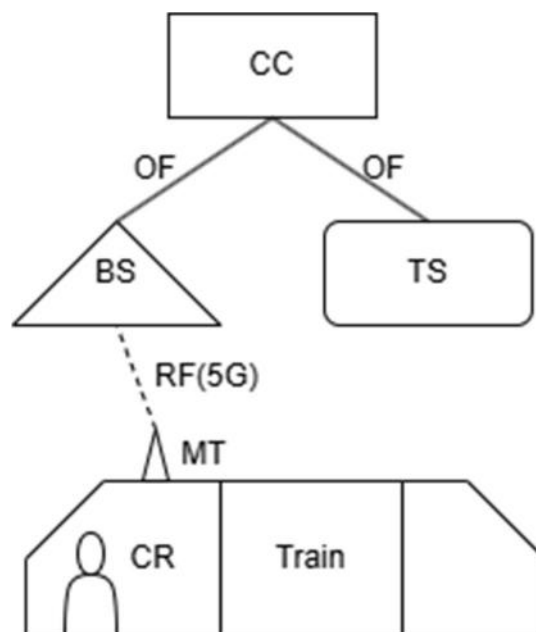


Figure 3.2 – General railway architecture.

Considering this architecture, the attacker has three main entry points to attack and exploit:

1. The Base Station.

2. The Control Room inside the train.
3. The network equipment inside the passenger carriages.

3.3 Control Centre Architecture

The architecture of the Control Centre, Figure 3.3, is designed to manage both operational and passenger services, ensuring safe and efficient railway operations.

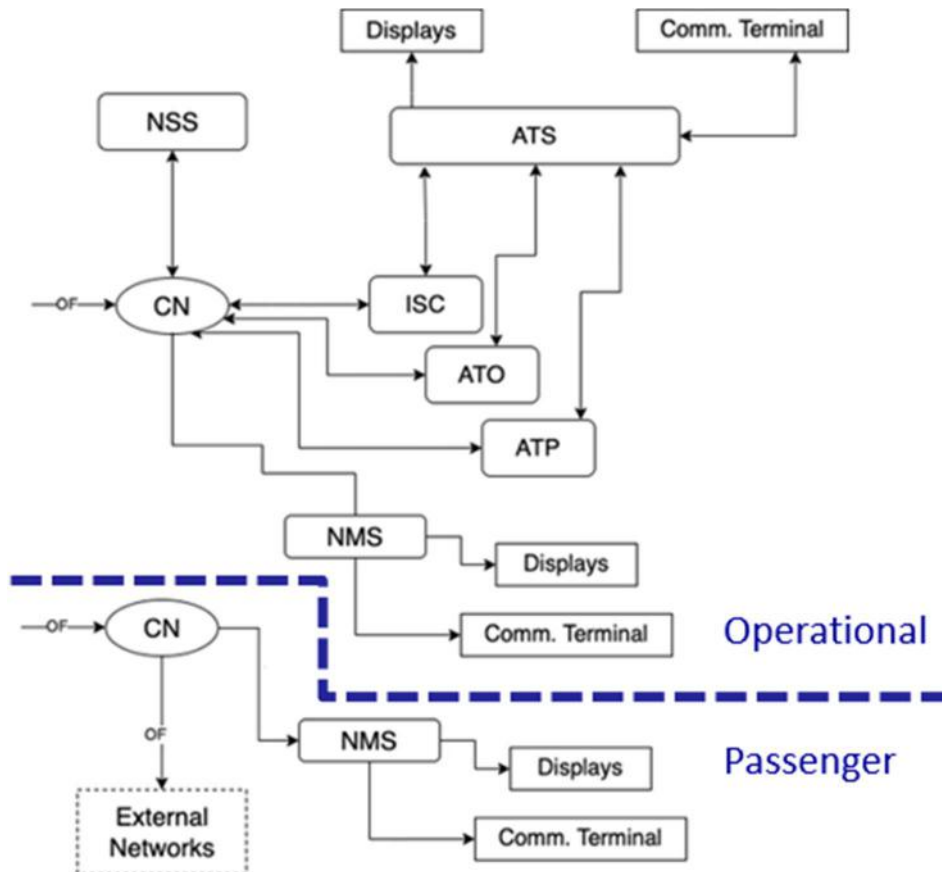


Figure 3.3 – Railway control centre architecture.

The segregation of services is maintained by having separate core networks for operational and passenger services.

- The Core Network (CN) is the central hub through which all information flows into the CC. It receives and processes data from various subsystems, ensuring that operational and passenger services are handled separately to avoid interference and enhance security.
- The Network Switching System (NSS) supports the CN by managing data flow between the core network and external systems. It performs switching functions to ensure efficient communication and data routing within the network.
- The Automatic Train Supervision (ATS) is responsible for overseeing train traffic. It monitors and controls train movements, track occupancy, and speed limits. It provides real-time data to train drivers, enabling them to make informed decisions while operating the train.
- The Automatic Train Operation (ATO) automates key train functions, such as acceleration,

cruising, and deceleration. Its primary purpose is to maintain the train's schedule and improve energy efficiency by optimising speed and movement automatically.

- The Automatic Train Protection (ATP) is a safety-critical system that ensures trains operate within defined speed limits. It automatically stops the train in emergencies or if there is a violation of safety protocols. This is crucial for preventing accidents and ensuring safe operations.
- The Interlocking System Centre (ISC) is responsible for preventing train collisions and accidents. It controls the movement of trains based on signals and ensures that routes are clear before allowing a train to proceed. It is a key safety component of the signalling system.
- Network Management System (NMS) is a software platform used to monitor, manage, and maintain the railway network. It ensures that both operational and passenger services are running smoothly by overseeing network performance, detecting issues, and initiating corrective measures as needed. It is equipped with an Intrusion Detection and Protection System (IDS/IPS).

The architecture clearly separates operational services from passenger services. This segregation is enforced through distinct core networks, preventing interference between the two types of services and enhancing overall system reliability and security. Each CN is connected to its own set of terminals and display systems to ensure efficient operation.

As mentioned before, the CC is not a vulnerable entry point for an attacker, meaning that an attacker cannot directly access or compromise the CC. For the attacker to affect the CC, he would need to gain access to another component of the network, the train itself for example.

3.4 Train Architecture

In this section, the train architecture is presented as a network of interconnected systems responsible for communication, security, and operations. The following sections explore its general structure, highlighting key components such as the driver's cabin, control rooms, and network connections. One approach to security involves physical segregation, where dedicated cables and hardware isolate critical and non-critical services. Another approach relies on logical separation, using VLANs to maintain security while sharing infrastructure. The architectures presented in this section were developed based on a reference model provided by HITACHI, illustrated in Annex A.

3.4.1 Train's General Architecture

The physical architecture of the train, as shown in Figure 3.4, consists of multiple interconnected systems designed to support communication, security, emergency services, and passenger information management. The architecture is structured into different sections, including the driver cabin and control room and the passenger carriages, ensuring that critical and non-critical services are properly managed and isolated. In this architecture, after communications arrive at the train, they are segregated physically, with different physical components for different types of service.

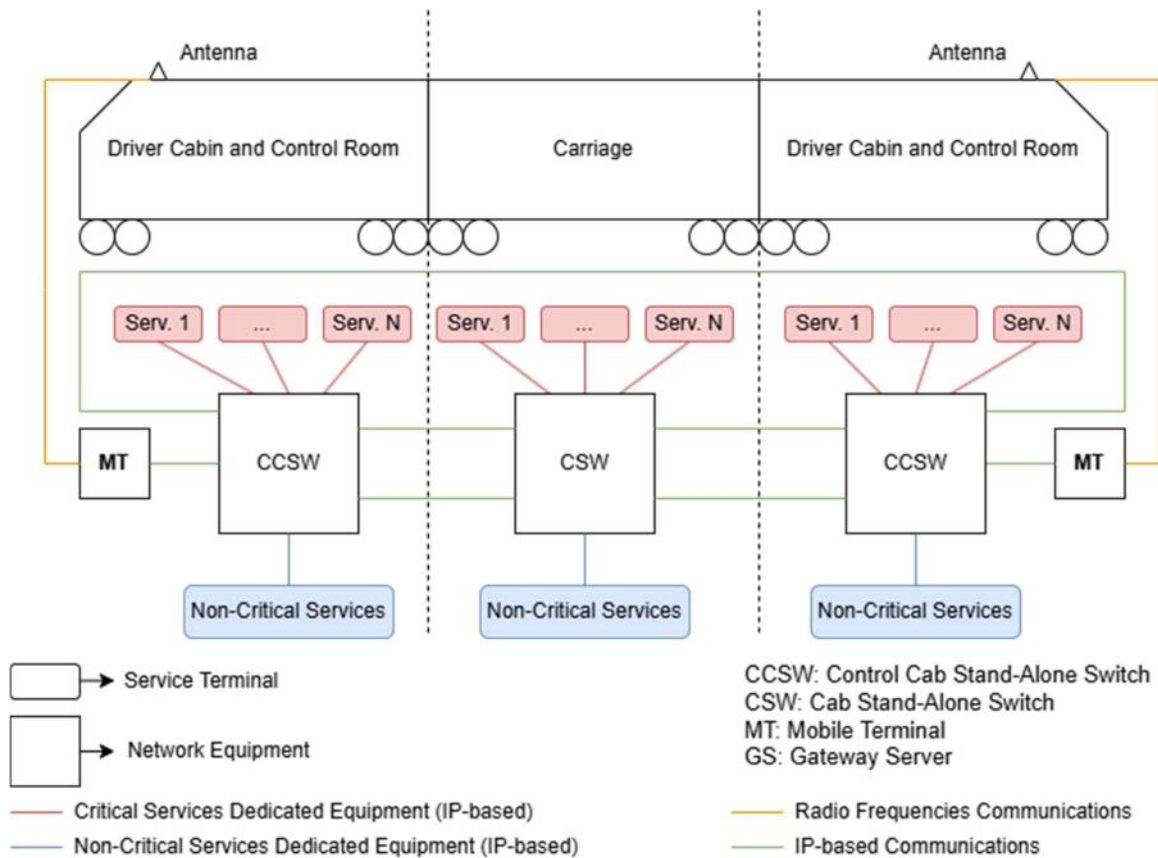


Figure 3.4 – Train architecture.

The train is symmetrical, meaning that there is a Control Room (CR) and an Antenna on both ends of the train. Both antennas are connected to each respective Mobile Terminal inside the CR, by cable. The CRs are inside the driver's cabin and both the CR and the driver's cabin should only be accessible by the driver himself. The driver's cabin is locked with a key designated to the driver and there is no motion sensor alarm that notifies when the door is opened.

Inside the CR, there is a Mobile Terminal and a Control Cab Stand-Alone Switch (CCSW), which is composed of many components, as shown by Figure 3.5:

- The Mobile Terminal (MT) serves as the primary communication hub between the train and the base station. It ensures real-time data exchange between the train and the control centres, providing critical diagnostics and operational data for efficient and safe operations. It is composed of an antenna outside the train, to help in the transmission and reception of signals, and its computing components inside the control room. The itself antenna has no safety features against physical attacks.
- The Gateway Server (GS) acts as an initial firewall and filter for incoming and outgoing communications. It distinguishes between critical and non-critical data, routing it to its specific services. It also facilitates efficient routing of data to the control centre.
- The operational Network Management System (NMS) monitors the performance of the train's communication systems, ensuring stable and secure operation of critical services. It evaluates network health, detects issues, and initiates corrective actions when needed. It is equipped with

an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) to help detect and prevent against attacks that pass undetected through the initial firewall.

- The Onboard Automatic Train Operation (ATO) system automates key train functions such as acceleration, deceleration, and maintaining the scheduled timetable. It uses sensors to gather real-time data and make decisions that reduce reliance on manual operation, improving both safety and energy efficiency.
- The Onboard Automatic Train Protection (ATP) system ensures that the train operates within predefined safety parameters. It prevents over speeding, collisions, and other hazardous situations by automatically triggering safety measures when necessary. ATP plays a vital role in maintaining the overall safety of the train's operation.
- The switches provide an additional layer of security and facilitate the internal networking of the train's operational systems, creating VLANs for each service. They forward data to the correct terminals, ensuring secure and efficient communication within the train.

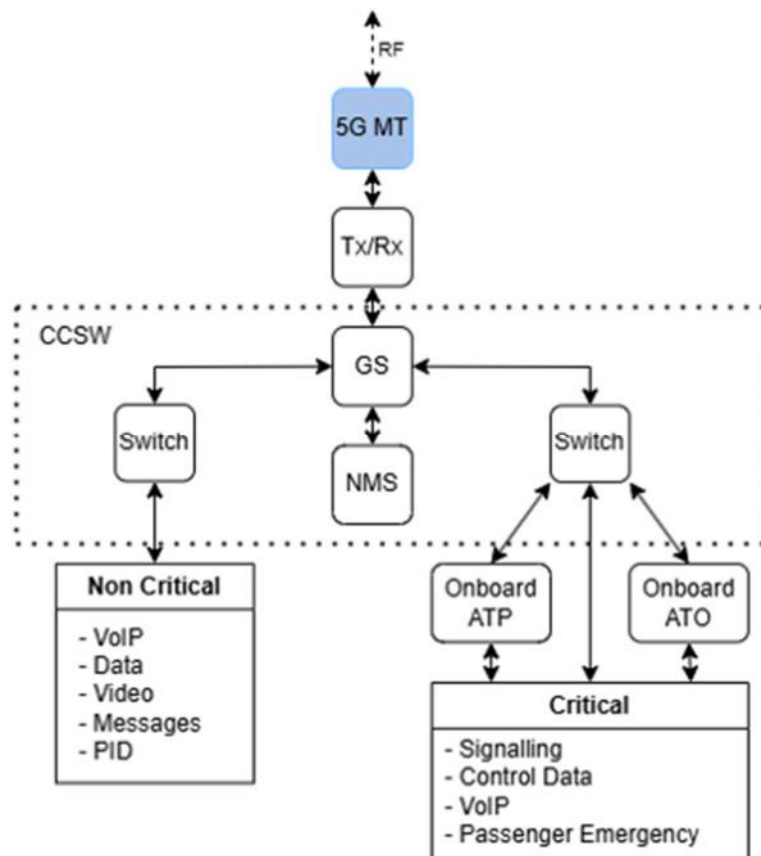


Figure 3.5 – Simplified control room architecture.

Communications from outside arrive to the Antenna and into the Mobile Terminal, where they are converted into IP-based communications and sent to the CCSW, where they are processed and routed to each respective terminal/network component. Throughout the other carriages of the train, there is one Cab Stand-Alone Switch (CSW) per carriage, hidden inside the roof, unlocked, that route communications to each service terminal.

Normally, only one CR is active while the other serves as a redundancy measure. The active one

generally is the one facing forward to the train's destination. The CR is turned on or off by the train's driver, who has a designated key. In rare occasions, it is possible for the active CR to be on the room opposite of the driver, in the case of a malfunction of the CR in the middle of the train's journey.

There are two possible scenarios that define which control room is active:

1. In Scenario 1, there is only one main CR which is always active, and the second control room only has redundancy purposes. When the driver reaches the end of the railway line, he turns the train around so that the main CR is facing forward.
2. In Scenario 2, only one CR is active at any given time. The active CR is determined by the train's direction of travel. When the train is moving in one direction, the forward CR is active, allowing the driver to control the train from that end. On the return journey, the train's driver, walks to the opposite side of the train and activates the other CR, enabling control from the other end.

Communication between Control Rooms at each end of the train is ensured by an IP Fixed Network, which physically connects the onboard services. Currently, this IP network offers only basic security through access control using ID and password. No IPsec protocol is implemented at the IP layer, meaning that communications are unprotected against interception and tampering. Although IPsec supports various configurations, including Transport and Tunnel modes, and protocols like AH or ESP, none are active in this setup. Thus, any encryption or integrity protection would need to be applied at higher layers, such as the transport (e.g., TLS) or application layer.

Additionally, the train's network employs a ring topology to ensure redundancy. This means that each carriage switch is connected to both its adjacent switches, forming a loop. In practice, this design greatly improves resilience. For example, if the switch in the first passenger carriage fails, the system can reroute traffic through the opposite side of the ring, maintaining communication with the second carriage and the rest of the train. Without this ring redundancy, a single point of failure in a carriage switch could isolate downstream components entirely.

3.4.2 Services with Physical Segregation

The first architecture, in Figure 3.6, focuses on physical segregation, where critical and non-critical services operate on separate dedicated cables and equipment. In this case, there are two dedicated cables that go throughout the train, one cable connects all critical switches, and the other, connects all non-critical switches, making sure that traffic is segregated until it reaches specific components.

After being processed at the MT, communications reach the GS, where they are inspected and classified as either critical or non-critical traffic and sent to each respective Switch. Since all inbound and outbound traffic for the train passes through the GS, the NMS, equipped with an IDS and IPS, continuously monitors network activity to enforce security policies. The GS maintains two distinct connections with the NMS. The primary connection allows the NMS to inspect traffic flowing through the GS, ensuring compliance with security protocols. The secondary connection is reserved for exceptional cases, enabling the NMS to issue alerts or intervene directly when a security anomaly is detected.

After leaving the GS, traffic is forwarded to the CCSW's switch, where it is segregated into four different VLANs and directed to the appropriate service terminals. This segmentation ensures that each type of communication remains isolated, ensuring that a compromised terminal associated with one service cannot interfere with or disrupt traffic belonging to another service. Each terminal has a dedicated port and cable to communicate with the switch.

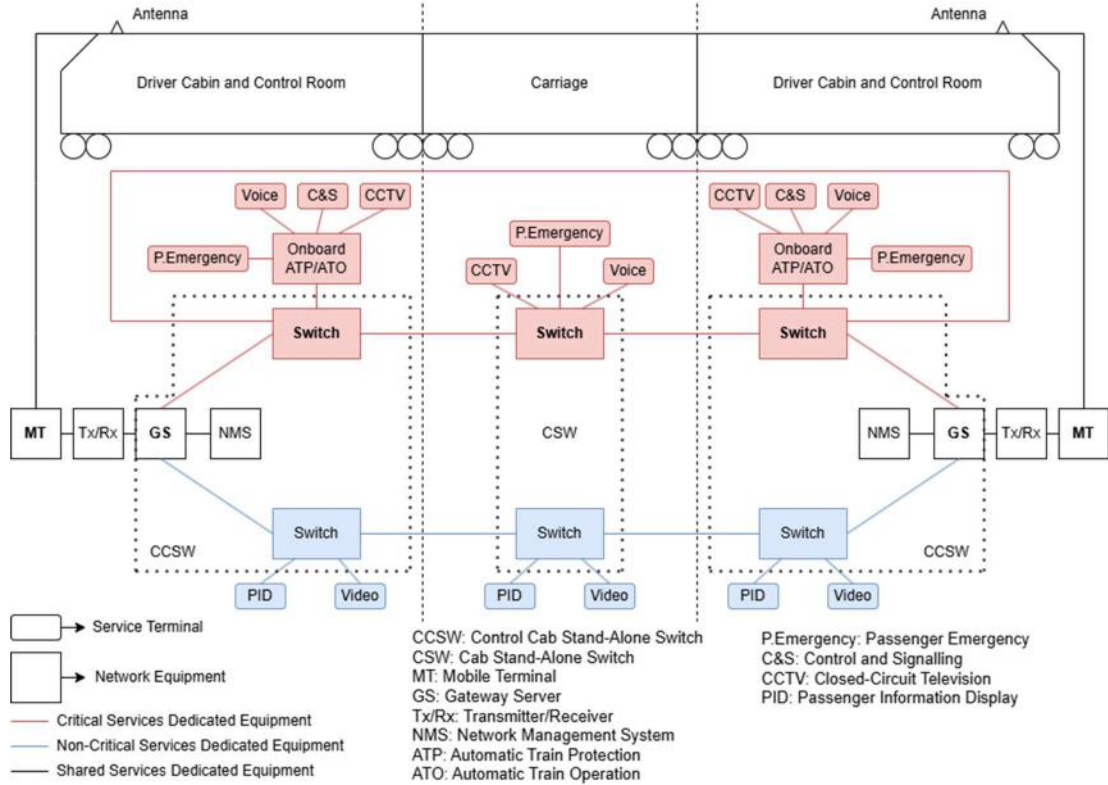


Figure 3.6 – Train’s physical architecture with a focus on physical segregation.

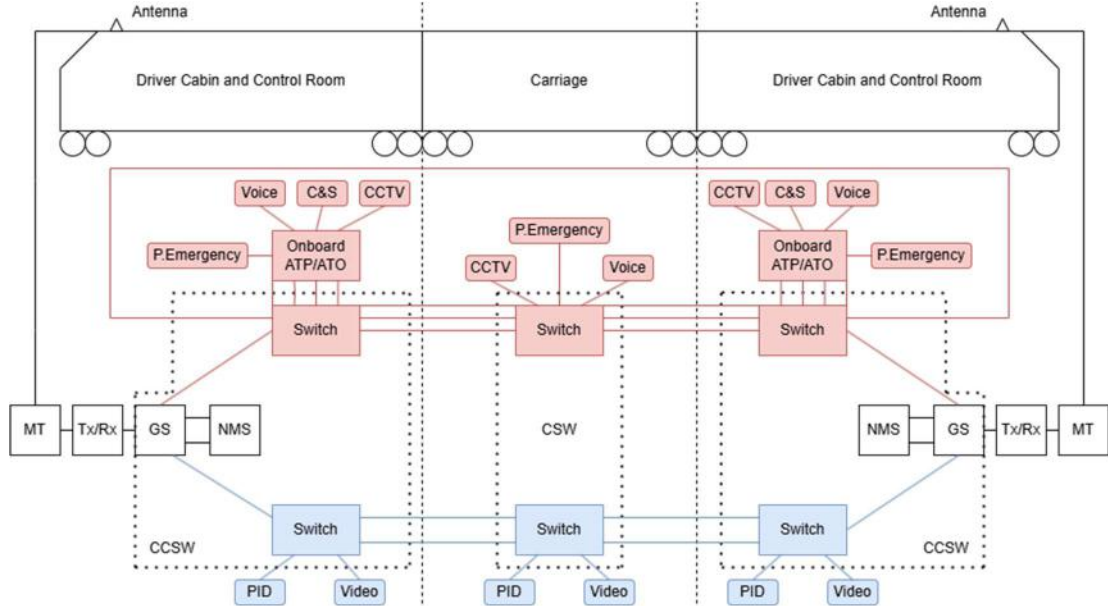


Figure 3.7 – Logical architecture with physical segregation (Notice how there are multiple VLANs).

To help understand how these components communicate with each other, a logical architecture is

shown in the above Figure 3.7.

Communications between the CCSW's switch and the CSW's switch are carried over a single physical cable configured as a trunk port, allowing multiple VLANs to remain segregated. Since the second switch provides three services, only three VLANs are needed, one for each service. The second switch then forwards each VLAN's traffic to its corresponding service terminal, and once again, each terminal has a dedicated port and cable to communicate with the switch.

3.4.3 Services without Physical Segregation

The second architecture, in Figure 3.8, follows a logical segregation approach, where services share some common infrastructure but remain separated through logical mechanisms such as VLANs and network policies. While critical and non-critical services converge on some equipment, their traffic is managed independently to maintain isolation.

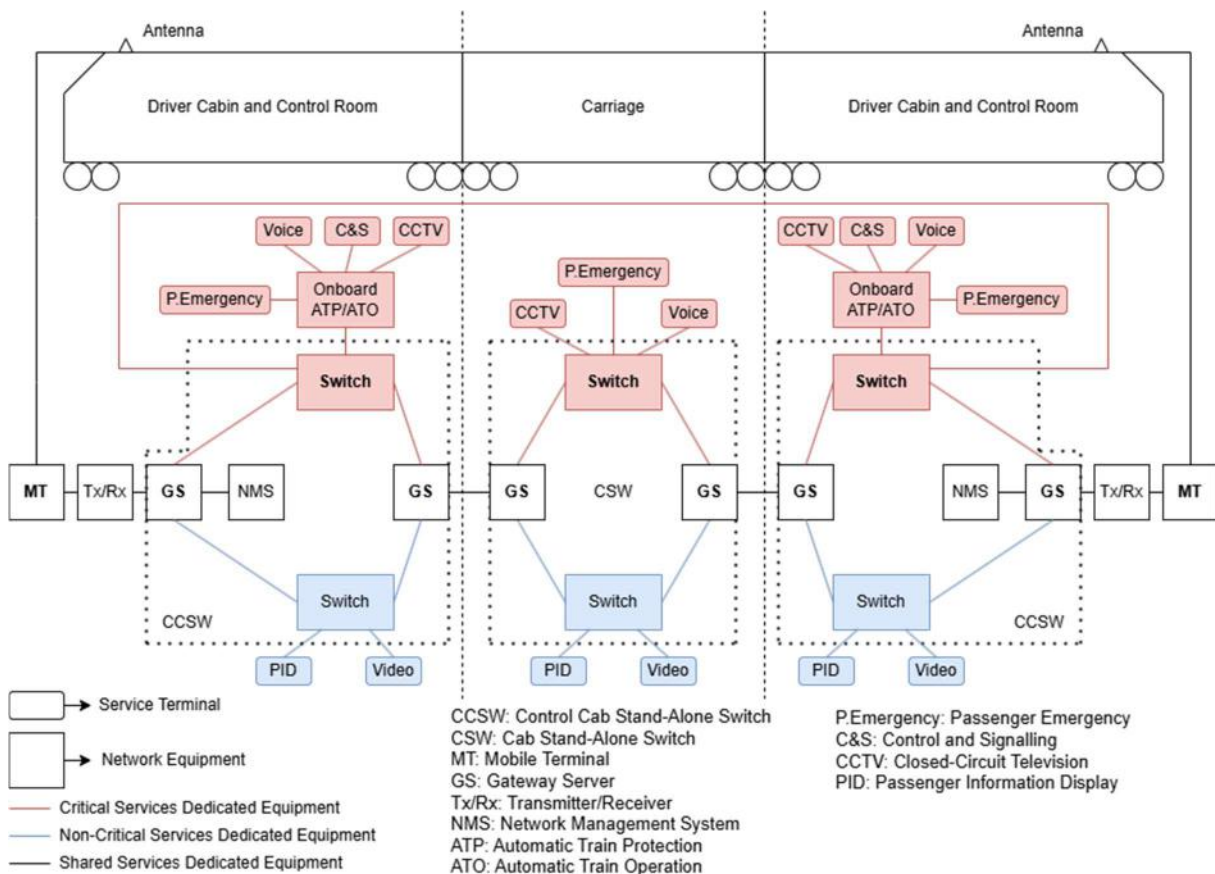


Figure 3.8 – Train's physical architecture with a focus on logical segregation.

Comparing this architecture to the one in Figure 3.6, with the use of a single cable to connect the CCSW to the CSW, additional gateway servers are added to handle the convergence and divergence of communications. These GSs ensure that critical and non-critical traffic remains segregated over the shared cable, but they also introduce additional security vulnerabilities. Each GS becomes a potential attack surface, increasing the number of components that must be secured and monitored.

The early communications process is like the one described in Figure 3.7, the difference resides in the

additional gateway servers. After leaving the CCSW's switch, where traffic is segregated into a single VLAN for each service, the VLANs are sent to a new gateway server. This gateway server aggregates both critical and non-critical traffic and forwards it to another new gateway server in the passenger carriage's CSW. At the CSW, the incoming VLANs are distributed to their respective switch, which forwards the traffic to the appropriate terminals, ensuring each VLAN reaches its corresponding service.

To help understand how these components communicate with each other, a logical architecture is shown in the following Figure 3.9.

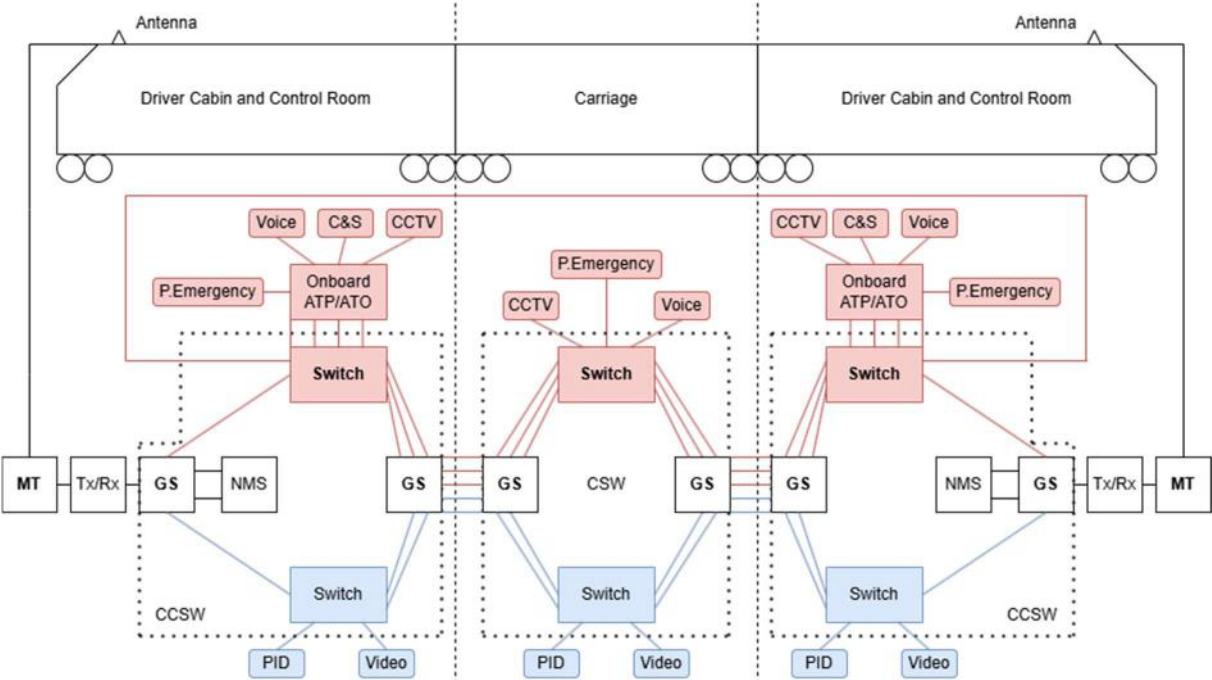


Figure 3.9 – Logical architecture without physical segregation (Notice how there are multiple VLANs).

3.5 Base Station Architecture

The architecture of the 5G base station or 5G gNB, Figure 3.10, is composed of three main components, the Antenna, the Radio Unit (RU) and the Distributed Unit (DU).

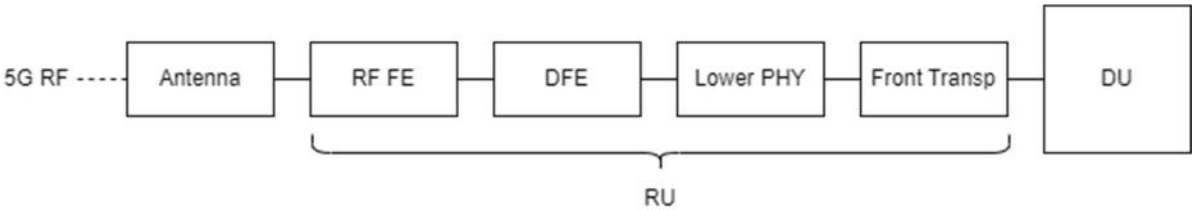


Figure 3.10 – 5G base station architecture.

The antenna is responsible for transmitting and receiving radio frequency signals. It sends out signals from the RU to user devices and receives signals from those devices for further processing.

- The Radio Unit is responsible for converting digital data into radio signals and vice versa, and it is composed of:
 - RF Front End (RF FE): The signal first enters the RF Front End from the antenna. It processes the raw analog signals, amplifying and converting them between analog and digital formats.
 - Digital Front End (DFE): After the signals are converted to a digital format, they enter the Digital Front End where they are further processed to ensure they are prepared for efficient transmission and meet the necessary spectral requirements.
 - Lower PHY Layer: The signal then moves to the Lower Physical (PHY) Layer, where operations involve modulating the signal for transmission, managing interference, and optimising it for the multiple antennas used in 5G systems.
 - Fronthaul Transport: Finally, the processed signal is sent to the Fronthaul Transport system, where it is encapsulated using various protocols for transmission to the Distributed Unit. Synchronisation components like IEEE 1588 ensure that timing is accurate, which is crucial for maintaining coordination between the RU and other network components.
- The DU handles real-time processing, such as scheduling, error correction, and resource management. It receives data from the RU and processes it before forwarding it to the Central Unit. The DU plays a crucial role in ensuring low-latency communication.

It is important to note that the RU is secured inside a locked cabinet, which only authorised personnel have access to.

Considering this architecture, only the antenna and the RU are vulnerable to attacks. The antenna is vulnerable to physical attacks while the RU is vulnerable to both physical and radio frequency attacks.

The secure cabinet which protects the RU's components is equipped with a motion sensor that activates an alarm whenever the cabinet is not properly opened with its key. The components inside the RU, more specifically, the RF FE, the DFE, the Lower PHY and the Front Transp, are protected with a personal identifier (ID) and password, meaning only authorised personnel can access them.

While the DU is also vulnerable, it cannot be compromised directly, meaning that an attacker would have to first gain access to the antenna or the RU to compromise the DU. Considering this, this component is not relevant in this thesis.

3.6 Chapter 3 Summary

Chapter 3 presents the architecture and services of modern railway communication systems, with a focus on security and critical infrastructure. Section 3.1 classifies railway services into operational and passenger services, further dividing them into critical and non-critical categories. Critical services such as signalling, emergency communication, VoIP, and CCTV are essential for safety and real-time coordination, requiring strict performance standards. Non-critical services like passenger Wi-Fi and

entertainment are not analysed further due to their lower security impact.

Section 3.2 introduces the high-level railway architecture, which includes the Control Centre (CC), Base Station (BS), Train Station (TS), Train, and onboard Control Rooms (CR). The BS and Train are considered vulnerable due to exposure to physical and radio-based attacks. The TS is not analysed in the thesis as it primarily serves non-critical functions. The attacker's main entry points are the BS, the onboard CR, and passenger carriage network components.

Section 3.3 details the internal structure of the Control Centre, which maintains separate core networks for operational and passenger services to ensure security and reliability. Key components include the Core Network, Network Switching System, ATS, ATO, ATP, ISC, and NMS. These systems handle train supervision, automation, safety enforcement, and network monitoring. Although the CC is not a direct target, it can be affected indirectly if another component like the BS or Train is compromised.

Section 3.4 presents the train's internal architecture, focusing on its communication network and security setup. The train is symmetrical with Control Rooms at both ends, each equipped with a Mobile Terminal and Gateway Server. Network traffic is segregated either physically (via dedicated cables) or logically (via VLANs), with both setups including IDS and IPS mechanisms. Communication between the CRs uses an IP Fixed Network, which lacks IP-layer encryption and relies on access control via IDs and passwords. A ring topology enhances fault tolerance by allowing traffic rerouting in case of switch failure.

Section 3.5 explains the structure of the 5G base station, composed of the Antenna, Radio Unit (RU), and Distributed Unit (DU). The RU is divided into subsystems that handle signal conversion, modulation, and transmission. The Antenna is physically vulnerable, and the RU can be targeted through both physical and radio-based attacks. However, the RU is secured in a locked cabinet with motion sensors and requires authentication for access. The DU is excluded from analysis, as it cannot be compromised directly.

Chapter 4

Security Assessment and Mitigation

Chapter 4 describes the performed security analysis to the railway communication system. It identifies potential physical and cyber threats, classifies vulnerabilities, and evaluates the associated risks. This chapter assesses the attack feasibility for different potential attackers and proposes countermeasures to mitigate the most critical risks.

4.1 Security Analysis Flow for Railways

Based on the architectures outlined before, a comprehensive analysis flow was defined to address the specific security challenges in railway communication networks. This flow, defined in Figure 4.1, serves as a guide to enhancing the security of railway communication systems by addressing each vulnerable component, from threat identification to vulnerability mitigation.

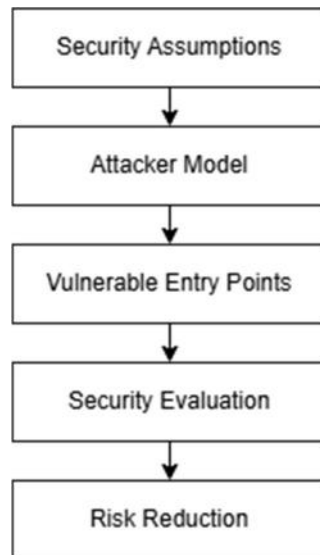


Figure 4.1 – Security analysis flow for railways.

This analysis flow consists of several key layers. At the top are the Security Assumptions. Here, the system's underlying security features and protocols are established, setting the foundation for evaluating vulnerabilities. These assumptions include the presumed security of components, communication links, and authentication mechanisms within the system.

The next layer involves the Attacker Model which defines the possible adversarial entities and their capabilities, allowing for a complete understanding of the types of attackers that may target the system. There can be more than one attacker, with different capabilities and resources.

Following this, the Vulnerable Entry Points are identified, which are potential weaknesses in the network that attackers could exploit. This includes physical access points, communication nodes, and software vulnerabilities that could serve as gateways for attacks.

The Security Evaluation layer is dedicated to the in-depth evaluation of each vulnerable point, using the STRIDE framework for the most common attacks. This analysis also includes the risk assessments, and the determination of how different threats could impact the system, factoring in both the likelihood of an attack and its potential consequences. This will be done using the DREAD framework. More information about these frameworks can be found in Section 2.2.1.

Finally, the model concludes with Risk Reduction. This layer outlines specific defensive strategies aimed at neutralising the threats identified and based on the DREAD analysis results. These countermeasures are tailored to address the unique vulnerabilities of the railway communication network, ensuring both operational resilience and security robustness.

4.2 Security Assumptions

This chapter establishes key security features and assumptions present in railway infrastructure and 5G communication networks. By defining these parameters, it is possible to delineate the potential scope of attacks and clarify the limitations of vulnerabilities that an attacker might exploit.

These are the assumptions for physical attacks:

1. The Control Centre, Figure 3.2, is secure, does not have unauthorised access either physically or through other means. It can only be compromised if an attacker gains access to the entire network through other means.
2. The Base Station, shown in Figure 3.10, is vulnerable to physical tampering due to insufficient protection.
3. The Control Room, shown in Figure 3.5, is vulnerable to a physical breach due to insufficient protection.
4. In the event of any suspicion activity that could endanger the train or its passengers, the driver is instructed to immediately halt all train operations and initiate a full shutdown.

Common throughout the entire network are optical fibre connections, which can be dug up and cut apart, causing disruption of the communications. This is not relevant to this thesis.

These are the assumptions for cyber and radio frequency attacks, which are tied up to 5G's inherent security features.

5. Communications between the train and the base station, Figure 3.2, are encrypted. It prevents any eavesdropping attacks.
6. Communications between the train and the base station, Figure 3.2, are authenticated. It hinders spoofing attacks and unauthorised accesses.

When specifically talking about the security features in the railway system, there are a few:

7. No unauthorised device can wirelessly connect to the network and the authorised devices are not allowed to receive foreign messages.
8. There is no internet access from the network. This eliminates a big source of possible malicious packets, which also means that phishing attacks are not possible.

Assumption 1 is based on the low likelihood of an attacker physically accessing the highly secure Control Centre, thus eliminating complex physical attack vectors against it and allowing a focus on more realistic attacks.

The assumption that base stations may lack sufficient physical security, Assumption 2, enables an exploration of risks associated with compromised equipment and tampering, which are plausible threats in this environment.

Although it is protected by a closed door, only accessible with a key, the control room cannot be assumed to be safe. In Assumption 3, by declaring that the control room is vulnerable to physical attacks, it allows to analyse scenarios where an attacker can break open this door with specialised tools and compromise it.

By instructing the driver to halt operations and shut down the train, in Assumption 4, this protocol minimises the risk of unauthorised control. It also prevents any potential misuse of onboard systems until security personnel can assess and address the situation.

In Assumption 5, encryption is assumed as it is a standard security measure in modern communication systems. This eliminates simple eavesdropping attacks from the analysis, allowing a focus on other attack vectors.

Like Assumption 5, in Assumption 6, authentication is also presumed to be in place because it is essential in secure communication systems, especially in mission-critical contexts like railways. This allows basic spoofing attacks to be disregarded.

In Assumption 7, robust access control and message filtering are assumed, which removes the possibility of unauthorised device connections or phishing attacks. This assumption simplifies the threat landscape, allowing a focus on attacks that originate within the network or through compromised authorised devices.

Many secure, closed networks, such as those in railway systems, are typically isolated from the public internet. Assumption 8 eliminates a broad spectrum of internet-based threats such as phishing attacks.

4.3 Attacker Model

An attacker is an individual, organisation, or nation-state that engages in malicious activities targeting another person, organisation, or rival state [57]. This section outlines the attackers that are relevant to this study and then provide a detailed description of the threats they may pose.

The attackers in this study are defined as either unskilled or skilled, called Attacker “Low-Skilled” and Attacker “High-Skilled”. The Attacker “Low-Skilled” is important to analyse physical attacks and is talked about deeper in the following section. He has common knowledge about telecommunications, network and hardware manipulation, and has low access to specialised tools and resources. The Attacker “High Skilled” is an expert who has the necessary resources, tools and knowledge to achieve his goal, whatever it may be. The following Table 4.1 shows both attacker’s capabilities followed by a short description of them.

Network configuration manipulation involves changing the settings of network devices like routers, switches, and firewalls. Hardware manipulation is the act of physically tampering with railway equipment, such as base stations or onboard communication systems. Unauthorised access refers to entering restricted railway systems, facilities, or networks without permission. This could mean accessing train control systems, surveillance networks, or maintenance infrastructure to interfere with operations or steal sensitive data. Eavesdropping is intercepting railway communications, such as train-to-control centre or vice versa. Physical breaching means illegally entering secure railway facilities and physical destruction is the intentional damage of railway infrastructure. Disabling alarm systems involves tampering with security mechanisms like intrusion detection systems, surveillance cameras, or

emergency alerts. Bypassing access control is the act of avoiding security mechanisms like keycards, biometric scanners, or login authentication to gain control over railway networks or operational systems. Packet injection refers to inserting modified or malicious data packets into railway communication networks.

Table 4.1 – Attacker’s capabilities

Capability	High-Skilled	Low-Skilled
Network configuration manipulation	✓	✗
Hardware manipulation	✓	✗
Unauthorised access	✓	✗
Eavesdropping	✓	✗
Physical destruction	✓	✓
Physical breaching	✓	✓
Disabling alarm systems	✓	✗
Bypassing access control	✓	✗
Packet injection	✓	✗

It is important to note that although the attacker has the beforementioned capabilities, it does not mean that is always successful in exploiting vulnerabilities. For example, even though he has eavesdropping capabilities, it does not mean that he is successful in getting unauthorised information, since said information could be encrypted.

4.4 Vulnerable Entry Points

Vulnerable entry points are interfaces or components within a system that can be exploited by an attacker to gain unauthorised access or cause disruptions. Considering the railways scenario, the attacker will look to exploit the network through its entry points [58], shown in the Figure 4.2 below.

The railway network has three main entry points for an attacker to try and exploit: the base station, the mobile terminal’s radio interface, and the network equipment and service terminals inside the train.

An attacker can gain access to the railway network through physical means or radio frequencies. The base station is vulnerable to both and so is the train, being physically vulnerable through the network components spread throughout the control room in the drivers’ cabin and the other carriages, and vulnerable through radio frequencies only through the mobile terminal.

It is also important to note that the compromise of a single component can serve as a pivot point for broader exploitation of the network. For example, if an attacker gains full access and control of the base station, they will obtain elevated privileges over the entire communication infrastructure.

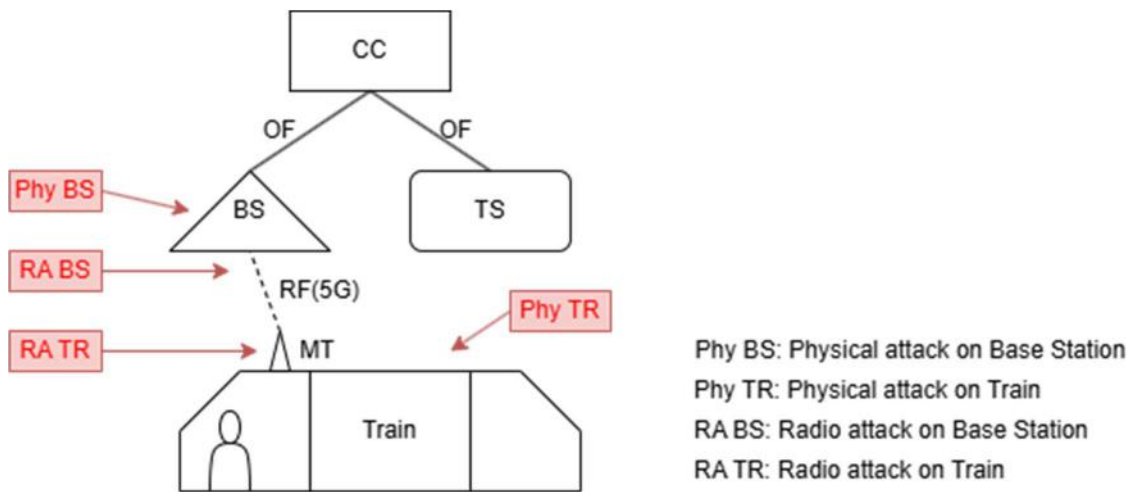


Figure 4.2 – Physical and cyber-attack entry points for a 5G railway network.

4.5 Security Evaluation

In the following sections, a detailed security analysis is conducted on key components within the railway communication network. Each component is evaluated based on its vulnerabilities, potential attack scenarios, and associated risks. The assessment considers both physical and cyber threats, examining how different attack vectors could impact the railway network.

4.5.1 Security Analysis Classification Methodology

The security analysis of the railway network will follow a top-down approach, beginning with the Base Station and progressing downwards to the train's components. This structure ensures that vulnerabilities at the highest levels, which could impact multiple components, are assessed first.

The security assessment can include both physical and cyber threats, structured based on the functionality and accessibility of components. For the physical security analysis, components will be grouped according to access pathways. The Driver's Cabin will include all components inside the cabin, as they are accessed in the same way by entering the secured control room. Any breach here would potentially compromise multiple systems at once. The Passenger Carriages will form another group, as all components in other train sections share the same access route through the carriages. For the cybersecurity analysis, components will be grouped by logical function. Service Terminals will be analysed together since they provide user-facing services throughout the train. Switches will be treated as a single group, as they control network connectivity and data flow within the train. Gateway Servers will be assessed separately, as they act as central points where critical and non-critical communications converge and diverge, making them high-risk targets for cyber threats. Additionally, the Mobile Terminal will be separated from the other components and analysed independently, as it is the only system on the train responsible for 5G communication and IP-based data exchanges. Given its role in handling external network connections, it represents a unique attack surface that must be assessed distinctly

from other onboard systems. This grouping is justified by practicality and risk factors. Physical security measures often rely on barriers and access control, meaning that if one component is compromised, others in the same physical space are at risk. Cybersecurity threats, however, typically exploit networked devices rather than physical presence, making logical grouping more relevant.

The analysis begins with a generic STRIDE table for each component, excluding Repudiation, which is not relevant in this context. Repudiation attacks refer to situations where an entity denies having performed an action, and the system lacks the means to prove otherwise. However, this type of threat is not relevant in this study, as the objective is not to attribute attacks to specific individuals or entities, but rather to identify vulnerabilities within the network and assess how they can be exploited and mitigated. The focus is on preventing and securing potential attack paths, not on tracing or proving responsibility after the fact. Next, a Tree of Threats is developed for each STRIDE category, detailing potential ways an attacker exploits vulnerabilities. These threats are classified using a colour system to indicate their feasibility and level of concern:

- Grey: the attack has an extremely low chance of being successful under normal conditions, making it unlikely to pose a practical threat. As a result, further analysis is not considered necessary.
- Yellow: like grey, but an analysis is conducted to evaluate the potential impact if the protective measures were to fail.
- Red: the attack is theoretically possible and requires further analysis to assess its risks and implications.

Based on these trees, attack scenarios describe how these threats are realistically carried out. For example, a physical attack on a base station could involve the attacker gaining proximity, bypassing alarms, and defeating access control systems to achieve full access. Finally, a DREAD analysis assesses some of the attack scenarios identified in the Tree of Threats. Since this analysis involves some level of subjectivity, scores will be assigned using a range-based classification:

- Very Low (1-2),
- Low (3-4),
- Medium (5-6),
- High (7-8),
- Very High (9-10).

To better support the threat evaluation process, a classification table has been created for each of the five DREAD categories. This table provides a set of scoring guidelines that define what constitutes low, medium, and high severity in a railway context. The classifications are based on practical considerations such as system impact, attacker capabilities, and service disruption scope. These criteria ensure consistency in assigning scores to each identified threat and facilitate a more objective risk prioritisation process.

The Table 4.2 below summarises the rationale used for scoring each DREAD dimension.

Table 4.2 – Scoring criteria for DREAD risk assessment categories.

Category	Very Low (1–2)	Low (3–4)	Medium (5–6)	High (7–8)	Very High (9–10)
Damage Potential	<ul style="list-style-type: none"> • Minor inconvenience • No lasting effects • No damage to equipment or services 	<ul style="list-style-type: none"> • Temporary disruption • Affects non-critical services • Easy to restore 	<ul style="list-style-type: none"> • Noticeable operational impact • Safety-critical services remain functional 	<ul style="list-style-type: none"> • Major disruption of services • Possible financial loss • May degrade safety systems 	<ul style="list-style-type: none"> • Catastrophic consequences • Risk to lives • Severe physical or infrastructure damage
Reproducibility	<ul style="list-style-type: none"> • Requires rare conditions • Highly situational • Difficult to repeat 	<ul style="list-style-type: none"> • Needs insider access or special tools • Hard to reproduce 	<ul style="list-style-type: none"> • Reproducible with planning • Requires moderate technical capability 	<ul style="list-style-type: none"> • Relatively easy with access • Tools are publicly available 	<ul style="list-style-type: none"> • Easily repeatable • Requires minimal skills • Automated tools widely available
Exploitability	<ul style="list-style-type: none"> • Multiple steps required • Needs privileged access • Extremely difficult 	<ul style="list-style-type: none"> • Requires deep system knowledge • Unlikely without inside help 	<ul style="list-style-type: none"> • Moderate difficulty • Needs some access and technical skills 	<ul style="list-style-type: none"> • Low barrier of entry • Executable with limited knowledge or tools 	<ul style="list-style-type: none"> • Trivial to execute • Basic skills or pre-built tools are enough
Affected Users	<ul style="list-style-type: none"> • Isolated impact • Affects only non-critical users or devices 	<ul style="list-style-type: none"> • Limited number of users affected • Non-essential services impacted 	<ul style="list-style-type: none"> • Affects several services or carriages • Noticeable disruption 	<ul style="list-style-type: none"> • Large number of users affected • Disruption to critical operations 	<ul style="list-style-type: none"> • Affects all users or key services • May cause service-wide outage or danger
Discoverability	<ul style="list-style-type: none"> • Very hard to find • Hidden from external view • Requires insider knowledge 	<ul style="list-style-type: none"> • Requires deep reconnaissance • Only visible with detailed system analysis 	<ul style="list-style-type: none"> • Detectable with moderate probing • May be inferred through behaviour 	<ul style="list-style-type: none"> • Obvious or partially documented • Low effort to identify 	<ul style="list-style-type: none"> • Publicly known • Easily spotted via inspection or open sources

The damage potential score reflects the expected impact on safety, service availability, and physical infrastructure, with higher scores indicating more severe disruption or risk to human life and equipment. Reproducibility measures how consistently an attack can be replicated. A highly reproducible threat poses greater risk as it can be consistently exploited with minimal effort under different circumstances, while threats that are difficult to reproduce may present lower immediate risk. Exploitability considers the technical difficulty and access level required to carry out the attack, where easily executed attacks using common tools or minimal knowledge are rated higher. The affected users score is based on the extent of the system impacted, with higher values assigned to threats that affect critical services or many users. Finally, discoverability measures how easy it is to detect the vulnerability; threats that are publicly

known or easily identified through basic inspection are rated with higher scores.

After the analyses are completed for each component, an attacker's perspective evaluation is conducted. This step provides additional insight by estimating how attractive each attack is from an adversary's point of view. This evaluation is structured using the following five categories:

- Risk: this represents the final risk level derived from the DREAD analysis for each scenario.
- Attacker Type: this indicates whether the attack could be performed by a low-skilled attacker, a high-skilled attacker, or both.
- Ease of Execution: this metric aggregates the Reproducibility, Exploitability, and Discoverability dimensions from the DREAD model.
- Attacker's Gain: This factor represents the potential benefit for the attacker, which is measured in terms of the financial loss caused to the company if the attack is successful. The higher the operational or infrastructural damage, the more attractive the scenario becomes from the attacker's point of view.
- Reputation Impact: this category estimates the damage to the company's public image if the attack and its results became known. Attacks involving simple destruction of equipment, such as vandalism, tend to have a lower reputation impact compared to cases where an attacker bypasses security mechanisms and gains unauthorised access to protected components, as the latter suggests deeper systemic vulnerabilities.

The following sections present the results of the analysis, with emphasis not only on the identified threats and risks, but also on the systematic application of the methodology to each component of the railway communication network.

4.5.2 Security Evaluation: Base Station

The STRIDE table, in Table 4.3, provides a classification of potential threats against the 5G base station, categorising them into Spoofing, Tampering, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege (EoP). Each threat describes an attacker's possible actions, such as impersonating a Mobile Terminal, modifying or intercepting data, overloading resources, or gaining unauthorised access to base station functions.

Table 4.3 – STRIDE table for the Base Station.

Spoofing	The attacker pretends to be a MT, sending malicious signals to the BS.
Tampering	The attacker modifies information passing through the BS.
Inf. Disclosure	The attacker discloses secret information known by the BS.
DoS	Exhausting the BS's resources.
EoP	The attacker gains access to any BS feature.

The Tree of Threats, in Figure 4.3, broadens the STRIDE table and visually represents the different attack vectors targeting the base station, illustrating how an adversary might compromise its integrity. The threats are further categorised based on realism, using different colours to indicate how feasible or practical each attack is in a real-world scenario.

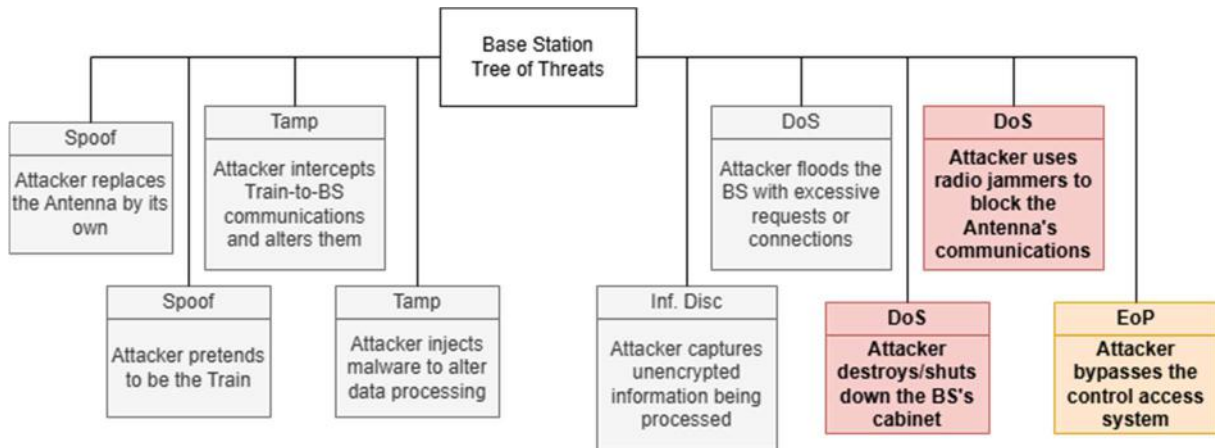


Figure 4.3 – Tree of Threats for the base station.

Some threats, like spoofing the train's identity, are theoretically possible but unrealistic due to 5G's mutual authentication, SUCI encryption, and integrity protections. An attacker would need to bypass strong cryptographic checks, break encryption, and compromise the train's secure SIM/eSIM, making such an attack infeasible without a major vulnerability in the network. 5G's security measures are further explained in Section 2.3.1.

Conversely, DoS attacks, like jamming or physically damaging the base station's hardware, are far more feasible. Jamming attacks can be executed using radio frequency interference, where an attacker transmits powerful noise signals on the same frequencies used by the base station, disrupting communication between the train and network. This is a well-known vulnerability in wireless networks and could be performed using commercially available jamming equipment. Another straightforward DoS method would be a physical attack on the base station's cabinet, which houses critical hardware. Simply destroying or cutting power to the base station would render it inoperative, leading to a complete loss of communication in the affected area.

While some attacks may seem unrealistic, insider threats remain a significant concern. A compromised technician with access to company systems could bypass security measures, disable alarms, and gain full control over the base station. Unlike external attackers, an insider might not trigger security alerts if they use authorised credentials to disable protections.

A base station can be attacked either through physical access or remote exploitation. Physical attacks involve direct tampering with hardware, while remote attacks rely on network vulnerabilities. The first scenario explores what happens when an attacker gains access to the base station's physical location. The second scenario examines threats that occur without physical access, focusing on network-based exploits.

The first scenarios in Figure 4.4 focuses on attacks where the attacker has direct physical access to the base station. The first barrier is the physical security of the site, such as locked doors, surveillance, and alarm systems. If the attacker is unable to bypass these, their attack is blocked, and their only alternative is to destroy the entirety of the physical components. If they manage to open a locked door, an alarm system should activate, alerting the control centre, which can then take protective measures such as dispatching security personnel or remotely shutting down critical functions to minimise damage.

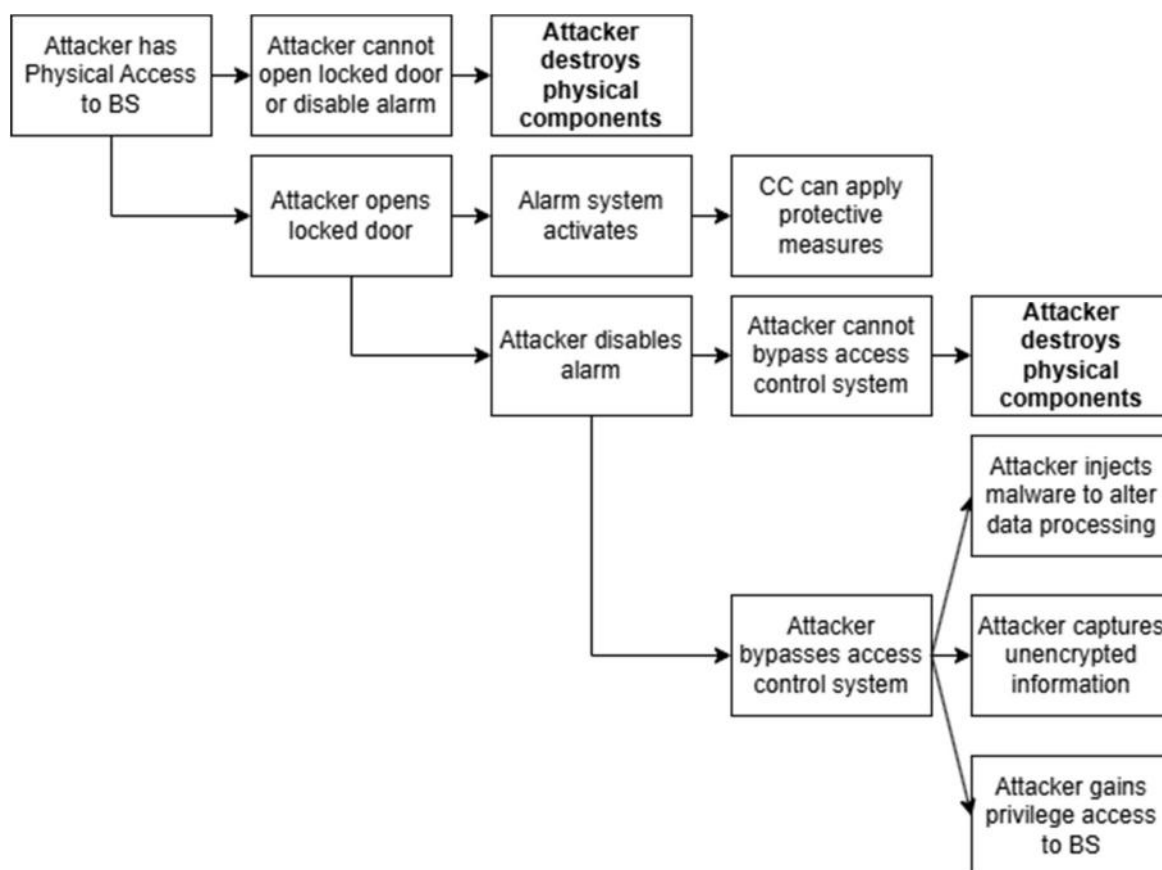


Figure 4.4 – Scenarios for physical attacks against a base station.

If the attacker successfully disables the alarm, but they cannot bypass the access control system, they can proceed with tampering. The most immediate risk is physical destruction of critical components, which can cause a complete DoS, disrupting all communications with the BS. This attack is simple but highly effective, requiring only basic tools to damage networking hardware, power supplies, or antennas.

If the attack is more sophisticated and involves bypassing access control mechanisms, it opens further risks. A skilled attacker could inject malware into the BS's systems, altering data processing and potentially affecting how it communicates with trains. They might also capture unencrypted information, leading to confidentiality breaches. The most severe case is if the attacker gains administrative privileges, allowing them to reconfigure or completely control the base station, creating persistent vulnerabilities or shutting down services at will.

The second scenarios in Figure 4.5 involves attackers who do not have physical access to the BS, meaning they must rely on remote exploitation. If security measures are weak or missing, more advanced attacks become feasible. An attacker could intercept and alter communications between the train and the base station, injecting false data, delaying commands, or manipulating operational signals. If proper mutual authentication and encryption protocols are not in place, they could also attempt to spoof the train's identity, making the BS believe it is communicating with a legitimate train. However, 5G's authentication mechanisms, SUCI encryption, and message integrity protection make identity spoofing highly unrealistic without a major security flaw.

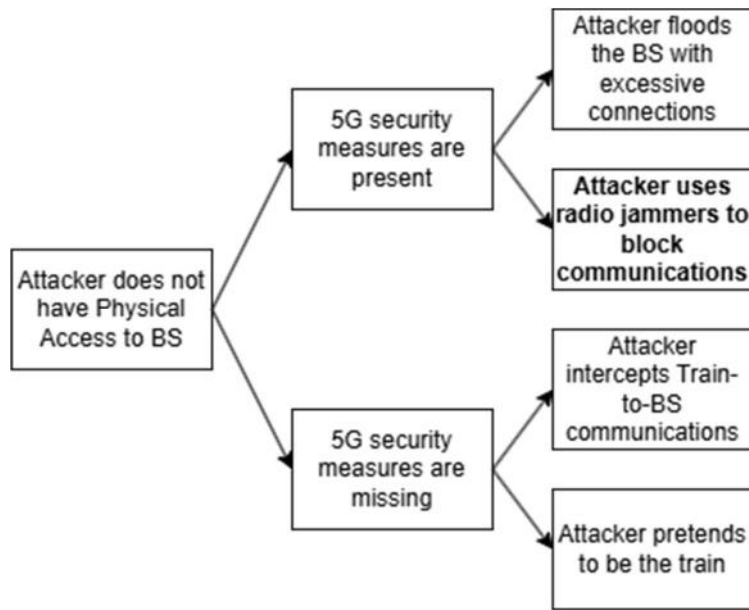


Figure 4.5 – Scenarios for cyber-attacks against a base station.

If the 5G security measures are properly implemented, most sophisticated attacks become much harder to execute. However, DoS attacks remain a major threat. An attacker can attempt to flood the BS with excessive connection requests, overwhelming its processing capacity and making it unable to handle legitimate communication. This kind of attack exploits the need for real-time responses in railway networks, potentially delaying train communications.

Another major remote threat is radio jamming, where an attacker uses high-powered radio signals on the same frequency as the BS, effectively blocking all wireless communication. This is a well-documented attack in wireless networks and can be executed with commercially available RF jammers.

As shown in the Tree of Threats and the scenarios, DoS attacks pose the most realistic and impactful threats to the base station. Only two types of DoS attacks will be analysed: physical destruction of equipment and radio jamming, as they are both feasible and capable of disrupting train-to-network communication. Other attack vectors, such as spoofing or tampering, are either impractical due to 5G security measures or require vulnerabilities that are unlikely to exist in a well-protected environment.

Table 4.4 shows a DREAD analysis that evaluates a physical attack on the BS, where an attacker gains access and damages or destroys critical components to disrupt communications between the train and the BS.

Table 4.4 – Physical attack on base station: damaging/destroying the components of the BS.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	High	High	Medium	Very High	High	High

The damage potential is rated at high. While disabling the BS completely cuts off communication between trains and the network, the railway system is designed with fail-safe mechanisms. Thanks to Assumption 4, if the train detects communication issues or unusual behaviour, the driver is required to

stop the train to prevent accidents. This reduces the risk of catastrophic consequences, making the primary effect of this attack operational disruption and equipment destruction rather than direct safety hazards. Reproducibility is rated at high, since the attack does not require advanced technical skills. With basic tools like hammers, cutting equipment, or explosives, an attacker with physical access can cause irreversible damage to the BS components. Exploitability is medium, as gaining access to the BS is difficult but not impossible. The BS is usually housed in restricted areas, protected by locks, alarms, and surveillance. The number of Affected Users is rated at very high, as the BS is a critical component in railway communication. If it is destroyed, all trains relying on it will experience communication failures, leading to delays, rerouting, and large-scale disruptions across the railway network. Discoverability is rated at high, meaning the vulnerability is somewhat known but not obvious. The location of the BS is generally not publicly advertised, but it can be identified through reconnaissance or insider knowledge. Once inside, the components that need to be destroyed are easy to identify, making it feasible for an attacker to execute the attack without requiring specialised knowledge. Overall, this attack scenario demonstrates a high-risk event with significant operational impact, but the presence of railway fail-safe mechanisms prevents immediate safety-critical failures such as collisions. The most severe consequences involve service disruptions, delays, and network failures rather than direct harm to passengers.

This DREAD analysis, in Table 4.5, evaluates a radio jamming attack on the BS, where an attacker disrupts communications by transmitting interference on the same frequencies used by the BS and trains. This attack does not require direct access to the BS but instead relies on proximity and sufficient transmission power to effectively jam signals.

Table 4.5 – Cyber-attack on base station: radio jamming.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Medium	Medium	Medium	Very High	High	Medium

The damage potential is rated at medium, meaning the attack prevents all train-to-network communication but does not directly harm physical infrastructure. While this could cause operational delays and logistical disruptions, the fail-safe mechanisms in railway systems ensure that trains halt operations when communication is lost, reducing the risk of accidents. Reproducibility is medium, as executing the attack requires proximity to the BS and a high-power radio transmitter capable of interfering with the targeted frequencies. While jamming devices are not commercially available in many regions due to legal restrictions, they can be custom-built or obtained illegally, making the attack feasible with moderate effort. Exploitability is also rated medium since an attacker must identify the BS’s general location and determine the specific frequency ranges used for train-to-BS communication. While this requires reconnaissance or technical knowledge, 5G frequencies are well-documented, and spectrum analysers can assist in pinpointing the right signals to jam. The affected users rating is very high, as the BS serves all trains within its coverage area. A successful jamming attack would disrupt all rail operations relying on that BS, leading to significant delays and widespread service interruptions. Discoverability is high, meaning the vulnerability is well-known, and radio jamming is a widely recognised

risk in wireless networks. However, determining the exact BS location and optimal attack positioning requires some knowledge, limiting its immediate accessibility. Overall, this attack scenario presents a moderate risk, primarily due to the large number of users affected and the potential for extended service disruptions. The risk score given to this attack is lower than the one in Table 4.4, since this attack is harder to perform.

In the next scenario, an attacker bypasses the access control system of the base station, gaining full administrative control. The DREAD analysis in Table 4.6 evaluates the potential impact if this attack were somehow successful.

Table 4.6 – Attacker bypasses access control system.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Very High	Very Low	Very Low	Very High	Very Low	Low

The damage potential is very high. If an attacker fully controls the base station, they could disrupt train-to-ground communications, manipulate signalling data, or disable the station entirely. This could result in major train delays, miscommunication between operators, and possible safety hazards. Assumption 4 only takes effect if the train or control centre detects anomalies in the network. However, in this scenario, the train perceives the network as functioning normally, meaning any malicious actions carried out by the attacker would go unnoticed. As a result, the assumption does not prevent potential damage to the network or train, as no safeguards would be triggered. The Reproducibility is very low since this attack is nearly impossible to repeat due to the protective measures in place. The BS system is equipped with an alarm that triggers if the station is physically opened, immediately notifying railway security teams. Additionally, access to the system itself requires an authorised laptop with valid credentials (ID and password), making unauthorised entry highly unlikely. Exploitability is also very low since executing this attack would require physical access to the base station, bypassing the alarm system, and stealing or compromising an authorised laptop with valid credentials. Even if an attacker possesses technical expertise, breaching multiple layers of security without triggering alerts is extremely difficult. The Affected Users rating is very high for similar reasons stated before in the other analysis. Discoverability is very low. The security mechanisms protecting the base station are not publicly documented, and the access requirements make it unlikely that attackers would even attempt this attack. Discovering and exploiting a weakness without detection is highly improbable. While the impact of this attack would be severe, the security measures in place make it nearly impossible to execute. The combination of physical intrusion alarms and strict access control requirements ensures that this scenario remains unrealistic. This attack is theoretically possible but does not represent a real-world threat in a well-secured railway network. However, it is still important to analyse this scenario, as the potential damage is extremely high. If an attacker were to somehow bypass these security measures, the consequences could be catastrophic, making it crucial to assess possible mitigation strategies even for highly improbable threats.

4.5.3 Security Evaluation: Mobile Terminal

The following Table 4.7, outlines STRIDE security threats against the train's Mobile Terminal. Spoofing allows an attacker to impersonate connected components, such as the Base Station or other network components. Tampering lets them modify data passing through the MT. Information disclosure exposes sensitive data stored or transmitted by the MT. DoS exhausts the MT's resources, disrupting functionality and EoP grants unauthorised access to MT features.

Table 4.7 – STRIDE table for the Mobile Terminal.

Spoofing	The attacker impersonates any component connected to the MT.
Tampering	The attacker modifies information passing through the MT.
Inf. Disclosure	The attacker discloses secret information known by the MT.
DoS	Exhausting the MT's resources.
EoP	The attacker gains access to any MT feature.

The Tree of Threats, in Figure 4.6, expands on the STRIDE table by visually representing attack vectors targeting the MT, showing how an adversary might compromise its integrity. The threats are categorised based on realism, using different colours to indicate the feasibility of each attack in a real-world scenario.

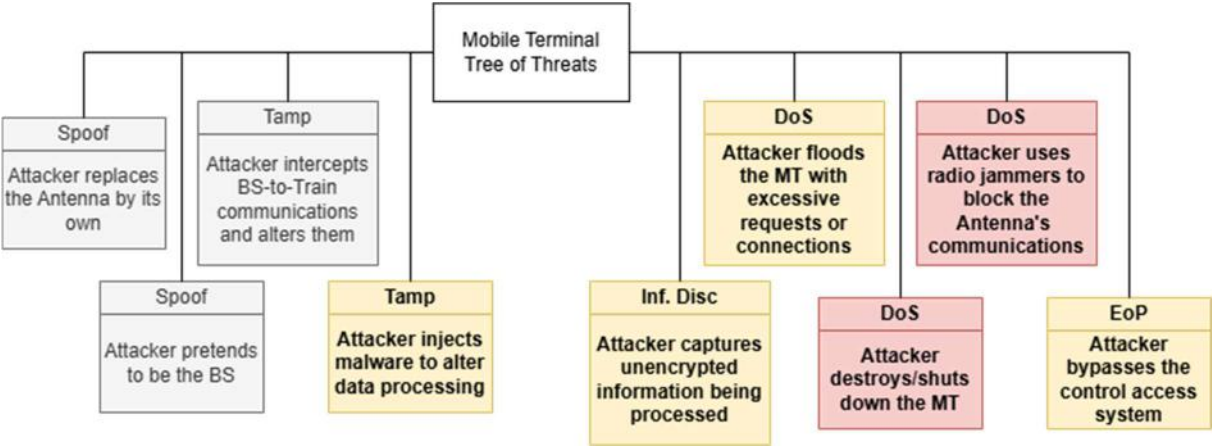


Figure 4.6 – Tree of Threats for the Mobile Terminal

Like the Base Station, 5G security mechanisms significantly reduce the risk of spoofing by implementing strong mutual authentication between the mobile terminal and the base station. This authentication process prevents unauthorised devices from acting as legitimate base stations or mobile terminals, blocking most spoofing attempts unless critical encryption keys or authentication mechanisms are compromised.

Although it will not be a focus of this thesis, an insider threat remains a major risk. A compromised worker with access to the network or security credentials could bypass access control systems without triggering immediate suspicion. If the attacker is an employee with valid access, they could exploit existing permissions to disable security mechanisms, manipulate network configurations, or introduce malware into the system.

The red-marked threats indicate the most feasible and dangerous attacks against the MT. A DoS attack

can flood the mobile terminal with excessive requests or connections, overloading its processing power and causing communication failures. Since railway systems rely on real-time data exchange, such an attack could delay operations or force manual interventions. Another DoS technique involves radio jamming, where an attacker uses signal interference to block the antenna's communication, preventing the mobile terminal from establishing or maintaining a network connection. This can be done using high-power RF transmitters that disrupt the specific frequencies used by railway communications. Additionally, an attacker can physically destroy or disable the MT, making it inoperable.

The following diagrams illustrate different scenarios in which an attacker can exploit vulnerabilities in the MT.

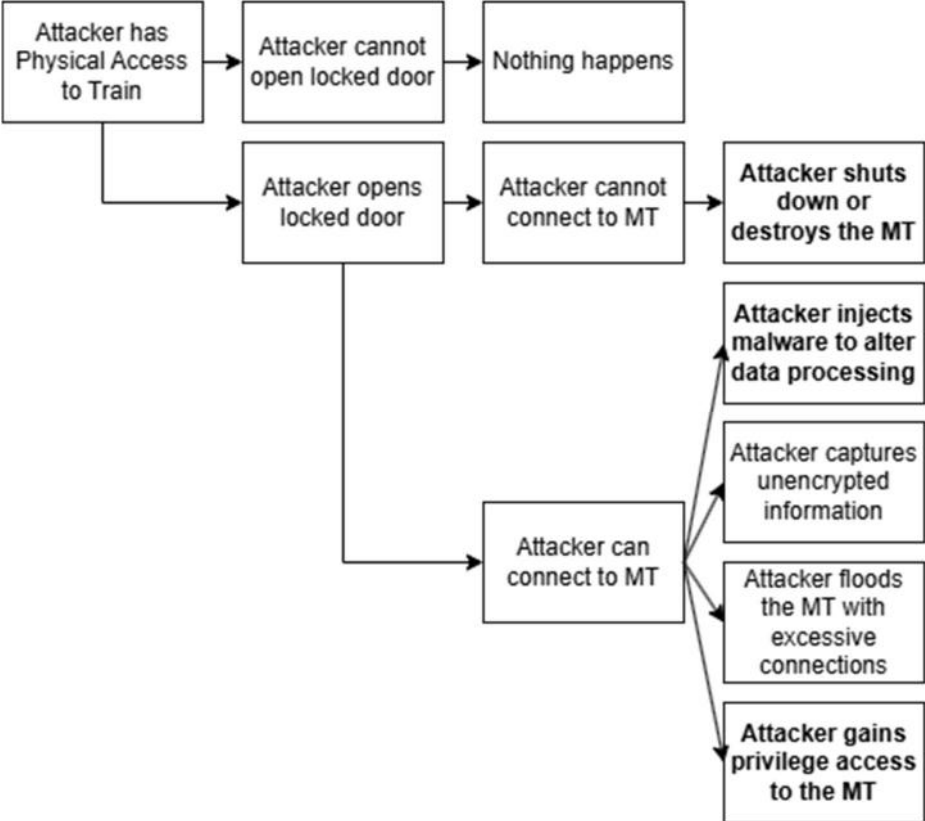


Figure 4.7 – Scenarios for physical attacks against the MT.

The first scenario, in Figure 4.7, illustrates how an attacker with physical access to a train could attempt to compromise the MT. If the attacker is unable to open the locked door, the attack is mitigated, and nothing happens. However, if the attacker successfully opens the door, they gain access to the train's internal components, including the MT. If the attacker cannot connect to the MT, he could still shut down or destroy it, disrupting train-to-network communication and forcing manual intervention. Otherwise, they could inject malware to alter data processing, which might manipulate communication systems, introduce false data, or interfere with critical operational commands. If unencrypted information is present, the attacker could capture sensitive data, including train location details, network credentials, or system logs. Another possibility is flooding the MT with excessive connections, executing a DoS attack that overwhelms the system, disrupts communications, and affects multiple trains depending on the compromised system. If the attacker gains privileged access, they could reconfigure settings,

execute unauthorised commands, or attempt to pivot into other connected railway networks.

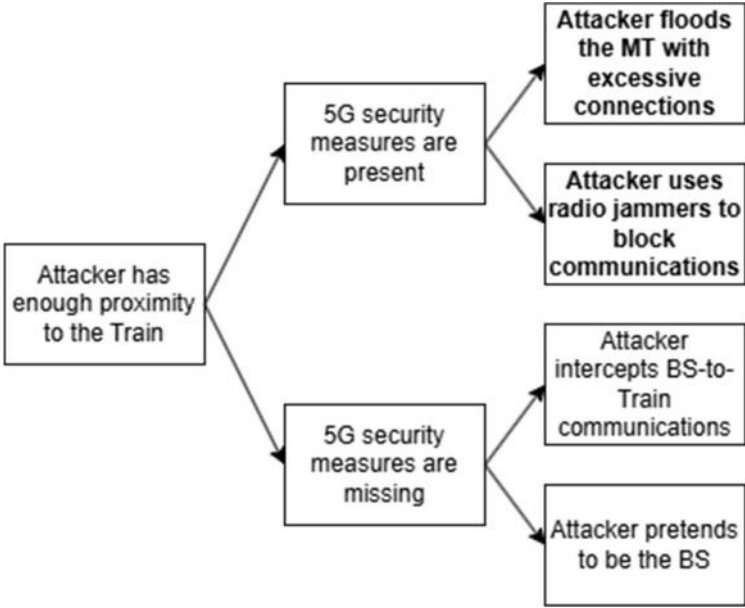


Figure 4.8 – Scenarios for cyber-attacks against the MT.

If 5G security measures are present, the attacker is limited to DoS attacks, such as flooding the MT with excessive connections or using radio jammers to disrupt communications, as shown by Figure 4.8. These attacks are most effective when the train is stopped at a station, as the attacker can stay nearby long enough to execute them. The attacker may also be inside the train, either as a passenger or a disguised worker, making it easier to deploy the necessary equipment discreetly. In some cases, the attacker might leave a small, embedded device or a radio jammer hidden inside the train, allowing them to execute the attack remotely without remaining physically present.

If 5G security measures are missing, the attacker has additional capabilities beyond DoS. Without strong authentication mechanisms, the attacker may attempt to intercept BS-to-Train communications, capturing unencrypted data exchanged between the train and the base station. Furthermore, the attacker could pretend to be the BS, tricking the MT into connecting to a rogue BS under their control. This could allow for man-in-the-middle attacks, where the attacker can modify or inject malicious data into the communication flow.

A DoS attack on MT, that aims to flood it with excessive connections, overwhelming its processing capacity and disrupting train-to-network communication. The impact of this attack is evaluated using the DREAD methodology in Table 4.8.

Table 4.8 – Cyber-attack on the MT: **flooding with excessive connections.**

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Low	High	Medium	Very High	Medium	Medium

The damage potential is revised to low, since the disruption of a single MT does not compromise the overall safety or operability of the train. In case the affected MT becomes unresponsive, control is

transferred to the redundant system in the opposite Control Room, ensuring continuity of operations. The attack may cause a temporary disruption, potentially triggering minor delays or requiring reconfiguration, but it is easily restorable and does not affect safety-critical services. The reproducibility is rated high because the attack is straightforward to execute using known DoS techniques and widely available tools, making it easily replicable once access to the communication channel is achieved. The exploitability is considered medium since the attacker needs knowledge of the MT’s communication protocols and access to sufficient network resources to sustain the attack, but physical access is not required. The affected users rating is very high, as all communications for that specific train are affected. The discoverability is medium because, while DoS attacks are well-known, pinpointing specific vulnerabilities in the MT requires some reconnaissance and understanding of railway network configurations. Overall, the DREAD assessment suggests that this DoS attack presents a moderate risk, primarily due to its operational inconvenience rather than long-term system damage.

A malware installation attack on the MT involves an attacker gaining access to the train, bypassing physical security, and successfully connecting to the MT to install a malicious program. This malware could alter data processing, impacting critical communication between the train and the railway network. The impact of this attack is evaluated using the DREAD methodology in Table 4.9.

Table 4.9 – Cyber-attack on the MT: **malware injection**.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Very High	Very Low	Very Low	Very High	Low	Low

The damage potential is rated very high because altering data processing on the MT could lead to the train receiving or sending incorrect information, potentially affecting operations in ways that could compromise safety. Without certainty about the train’s safety mechanisms, the risk includes the possibility of incorrect signalling, loss of communication with control centres, or failure to respond to emergency situations, which could result in catastrophic consequences. The reproducibility is rated very low since the attack requires multiple steps, including forcing entry into the locked driver’s cabin, remaining undetected, and successfully installing the malware. While the installation process itself may be simple, bypassing security measures without alerting personnel makes it significantly more difficult to execute. The exploitability is assessed as very low because the attacker must not only gain physical access but also connect to the MT, navigate any authentication barriers, and inject the malware while avoiding detection. The affected users rating is very high since all users would be affected. The discoverability is rated low because the attack requires specialised knowledge of the MT’s architecture, physical access procedures, and the ability to breach security unnoticed. If detected during the break-in, the attack would be completely neutralised as the train would immediately stop. The analysis indicates that installing malware on the MT poses an extreme operational and safety risk, as data manipulation could disrupt railway communications and lead to potentially catastrophic consequences. The difficulty of executing the attack without detection serves as a key mitigating factor, making it significantly harder to reproduce in a real-world scenario, which gives this threat a low risk overall.

4.5.4 Physical Security Evaluation: Train

Table 4.10 classifies physical security threats to train components using STRIDE. Spoofing involves impersonating authorised personnel to gain access. Tampering refers to altering information passing through components. Information Disclosure covers exposing sensitive data. DoS targets exhausting resources or shutting down components. EoP allows unauthorised access to system features.

Table 4.10 – STRIDE table for the train’s components.

Spoofing	The attacker impersonates any authorised personnel.
Tampering	The attacker modifies information passing through the components.
Inf. Disclosure	The attacker discloses secret information.
DoS	Exhausting the component’s resources or shutting it down.
EoP	The attacker gains access to any component feature.

The Tree of Threats, in expands on the STRIDE table by visually representing attack vectors targeting the MT, showing how an adversary might compromise its integrity. The threats are categorised based on realism, using different colours to indicate the feasibility of each attack in a real-world scenario.

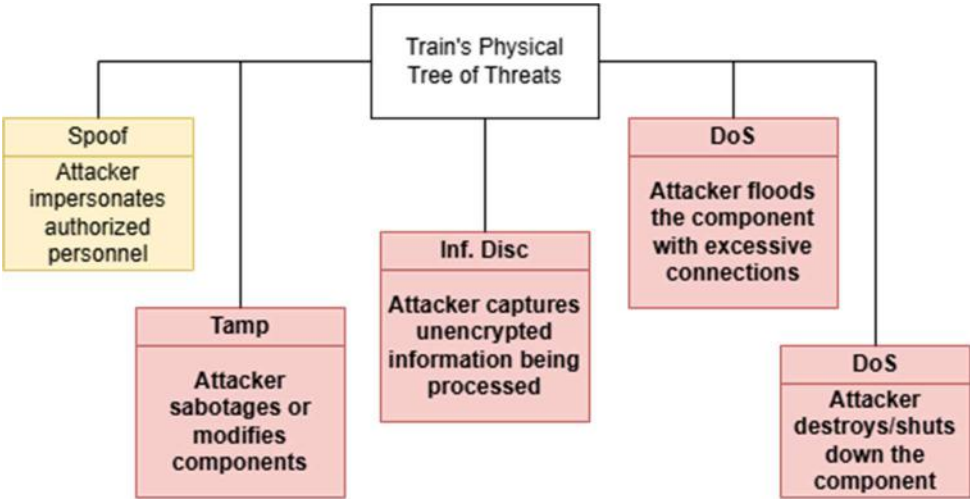


Figure 4.9 – Tree of Threats for the train’s components.

The attacks shown in yellow represent threats that are feasible if an attacker successfully impersonates authorised personnel. In the passenger carriages, components are unprotected, meaning an attacker dressed appropriately as maintenance staff could work on them without raising suspicion from regular passengers and he would go unnoticed. This makes impersonation a practical attack vector for accessing and tampering with these components. However, in the driver’s cabin, components are physically secured behind a locked door, making access through impersonation impossible unless the attacker bypasses the physical barrier. Because of this distinction, impersonation-based attacks are more likely to succeed in passenger carriages but not in the driver’s cabin. Once again, DoS attacks need analysis, as they are performable by any attacker.

The two following scenarios illustrate different attack approaches: one requiring the attacker to bypass a locked door to access the driver's cabin, and the other relying on locating and accessing hidden but physically unprotected components in the passenger carriages.

The first scenario, in Figure 4.10, represents an attack where the attacker must bypass a locked door to access the driver's cabin and its components. If the attacker fails to open the locked door, no further action can be taken, and the attack is unsuccessful. However, if the attacker manages to open the door, they gain direct access to critical train components. From there, the attacker can shut down or destroy a component, sabotage its functionality, capture unencrypted information, or flood it with excessive connections to cause a denial-of-service attack.

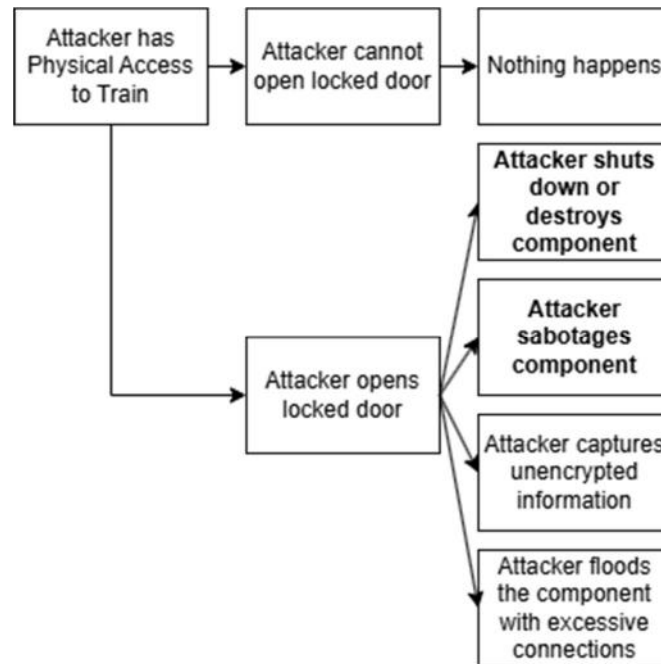


Figure 4.10 – Scenario for physical attack on the components inside the driver's cabin.

The second scenario, in Figure 4.11, describes an attack in the passenger carriages, where the attacker must locate and access hidden components.

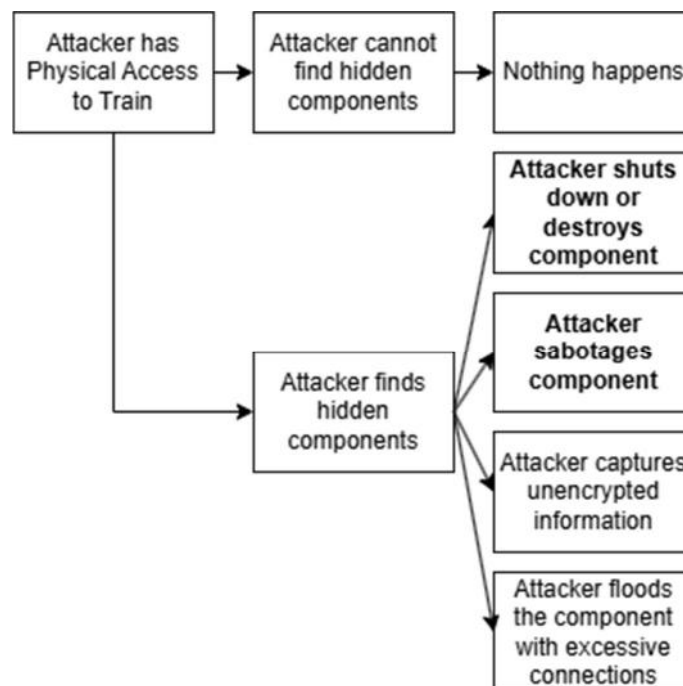


Figure 4.11 – Scenario for physical attack on the components inside the passenger's carriage.

These components are placed inside the roof of the train, but they can be accessed with a simple push. If the attacker fails to find the components, the attack is unsuccessful, and nothing happens. However, if the attacker identifies and accesses these components, they can perform the same range of attacks as in the first scenario.

The following DREAD analyses compare the physical security risks of destroying a switch inside the driver’s cabin versus destroying a switch in the passenger carriage. The key difference lies in accessibility and impact. In the driver’s cabin, the switch is protected. In contrast, the switch in the passenger carriage is physically unprotected, accessible with a simple push, making it much easier to target. by a locked door, meaning an attacker must first bypass this barrier before gaining access.

A DREAD analysis of destroying the switch in the driver’s cabin evaluates the impact of an attacker gaining access to the secured area and physically damaging the switch using simple tools, shown in Table 4.11.

Table 4.11 – Physical attack on the driver’s cabin: destroying/damaging the switch.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Low	Medium	High	Very High	Medium	Medium

The damage potential is low, as although the switch controls services like Control and Signalling, Passenger Emergency, and CCTV, the system is designed with redundancy. If one driver’s cabin becomes inoperable, the train can still be operated from the opposite cabin, maintaining control and communication capabilities. The incident would result in a temporary disruption of non-safety-critical functions and may require manual interventions or delay handling, but safety systems remain fully operational. The reproducibility is medium since the attack can be easily replicated using basic tools like a hammer, but the attacker would still need to perform the attack undetected by security personnel. Once an attacker breaks into the locked driver’s cabin, destroying the switch requires no specialised knowledge, making it a straightforward attack to execute repeatedly. The exploitability is also high because forcing entry into the cabin and damaging the component does not require technical expertise. Once inside, an attacker only needs physical access to the switch to destroy it, making this attack highly feasible if the attacker can bypass the physical barrier. The number of affected users is very high, as the switch manages critical functions that impact both passengers and railway operators. The discoverability is medium, since identifying the location and function of the switch inside the driver’s cabin is not that easy for an attacker without prior knowledge of the train’s architecture. Overall, this attack presents a moderate operational risk, mostly due to service interruptions and potential equipment loss, while safety-critical functions remain unaffected.

A DREAD analysis of destroying the switch in the passenger carriage evaluates a similar attack in an easier-to-access location, shown in Table 4.12.

Table 4.12 – Physical attack on the passenger carriage: destroying/damaging the switch.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Low	High	High	Low	Medium	Medium

The damage potential is low, since the switch primarily handles Passenger Emergency and CCTV systems. Destroying it would disable emergency response functions and surveillance, reducing passenger security for that specific carriage, but it would not affect train control or movement. The reproducibility is high because the switch is hidden inside the roof of the train but can be accessed with a simple push. Once located, it can be easily destroyed using basic tools, making it an attack that can be repeated without difficulty. The exploitability is also high since no security barriers prevent access to this component. An attacker does not need to bypass locked doors or override authentication mechanisms, meaning that simply knowing the switch’s location is enough to execute the attack. The number of affected users is low, as this attack would only impact passengers inside that specific carriage. The discoverability is medium, as an attacker would need to know the train’s internal layout and where to find the hidden switch. However, with prior reconnaissance or insider knowledge, locating the component would not be difficult. This attack represents a moderate security risk, primarily affecting passenger safety rather than train operations. Its feasibility is high due to easy access and minimal technical requirements, but its impact is limited to the affected carriage rather than the entire train.

4.5.5 Cyber/Logical Security Evaluation: Train

This section evaluates the logical and cyber security of the components within the train, focusing on potential vulnerabilities that could be exploited if an attacker gains access to these systems. As discussed earlier in the thesis, the components are split into groups based on their specific functionalities to provide a structured and comprehensive assessment. The components inside the train communicate through a private cabled network, which limits access strictly to those who can physically connect to this network. The physical security of these components and the means through which an attacker could gain access have already been addressed in Section 4.5.4. Therefore, this section focuses exclusively on what can be achieved logically or through cyber means once access to these components is obtained.

The Gateway Server, located inside the locked driver's cabin, is responsible for segregating and forwarding both critical and non-critical traffic. A potential vulnerability arises if an attacker gains access to this component. Traffic injection attacks involve inserting malicious or false data packets into the communication stream. If successful, such attacks could mislead safety systems, delay critical commands, or cause unauthorised actions. The following DREAD analysis in Table 4.13 evaluates the risk posed by traffic injection attacks on the Gateway Server.

Table 4.13 – Cyber-attack on the Gateway Server on the driver’s cabin: traffic injection.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Very High	Low to Medium	Very Low	Very High	Low	Low

The impact of such an attack is significant, especially for critical traffic, which gives this factor a score of very high. If a vulnerability is discovered, an attacker could repeatedly inject traffic using the same method until detected. However, the requirement for physical access to the driver's cabin highly reduces the likelihood of repeated attacks, resulting in a reproducibility score of very low. Alternatively, if an

attacker manages to install malware on the Gateway Server, it could allow remote execution of traffic injection attacks without requiring physical access. This scenario would significantly increase reproducibility, raising the score for this factor to high. Exploiting this attack would require bypassing physical security measures, such as the locked door of the driver's cabin, before even attempting to circumvent the network's IPS and IDS systems inside the network management system. This additional layer of security makes the exploitation more challenging, which is reflected in an exploitability score of very low. The attack can affect all communications passing through the Gateway Server, potentially disrupting all passengers and systems that depend on critical communications giving it a very high score. The fact that the Gateway Server handles both critical and non-critical traffic might suggest potential attack vectors. However, the physical security of the driver's cabin makes it less likely for an attacker to easily discover and study this vulnerability directly. This leads to a discoverability score of low.

Overall, the risk of traffic injection attacks on the Gateway Server inside the driver's cabin is low. The main risk factors stem from the potential damage and the number of affected users if an attack were successful. The presence of a locked cabin and the network management systems highly mitigates the risk by highly reducing both exploitability and discoverability.

Considering the architecture in Figure 3.8, there are also Gateway Servers spread throughout the passenger carriages, which could also be vulnerable to injection attacks. The following DREAD analysis in Table 4.14 evaluates the risk posed by traffic injection attacks on the Gateway Server on the passenger carriages.

Table 4.14 – Cyber-attack on the Gateway Server on the passenger carriage: traffic injection.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Very High	Medium	Low	Very High	Low	Medium-High

The damage potential is rated very high, as the Gateway Server is directly connected to switches in the driver's cabin that manage critical services such as control and signalling. An attacker leveraging the more accessible Gateway Server could inject a malicious program into the switch, potentially gaining control of these services. The reproducibility is assessed as medium, requiring prior knowledge of the train's internal layout and some level of planning to avoid detection during periods of low activity inside the train. The exploitability is scored as low, since the attack depends on deep knowledge of vulnerabilities in the Gateway and Switch components, as well as a solid understanding of their communication protocols. The affected user's category receives a very high score, as disruption of the Gateway Server affects all systems relying on train-to-ground communication and internal coordination. Finally, discoverability is low, as the vulnerability is not obvious and would likely require detailed system documentation or technical reconnaissance to identify.

Although the exploit requires significant technical expertise, the high damage potential and broad user impact, combined with the increased physical exposure of the component, raise the risk profile. Mitigating this vulnerability would require either physically securing access to the component or isolating its influence on safety-critical systems.

Like the gateway server, an analysis for traffic injection attacks is also made for the switches throughout the train. The DREAD analysis for traffic injection attacks on the switches evaluates the risk posed to two different scenarios: one where the switch is located inside the driver's cabin, Table 4.15, and another where it is located inside the passenger's carriages, Table 4.16. The switch inside the driver's cabin handles critical services, including Control and Signalling, while the switch inside the passenger's carriages only manages CCTV, Passenger Emergency, and Voice services.

Table 4.15 – Cyber-attack on the driver’s cabin switch: traffic injection.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Very High	Low to Medium	Very Low	Very High	Low	Low

Table 4.16 – Cyber-attack on the passenger’s carriage switch: traffic injection.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Very High	Medium	Medium	Very High	Low	Medium-High

The damage potential for traffic injection on the driver's cabin switch is rated very high, as compromising control or signalling data could result in serious operational disruptions, unauthorised command execution, or, in the worst-case scenario, safety incidents. Although the passenger carriage switch does not manage control or signalling directly, it is directly connected to the driver’s cabin switch, meaning that a compromise of the former could serve as an entry point to attack the latter. This escalation risk raises the damage potential of the passenger switch from medium to very high, since it can indirectly threaten critical systems.

In terms of reproducibility, the switch inside the driver’s cabin benefits from physical security provided by a locked door and cabinet, making repeated attacks less likely and justifying a very low score. However, if initial access is achieved and malware is installed, remote re-use of the attack becomes feasible, increasing reproducibility over time. For the passenger carriage switch, the lack of physical security means the attacker can access the component easily, especially during low-occupancy periods, resulting in a high reproducibility score.

The exploitability also varies. Gaining access to the driver’s cabin switch requires bypassing physical locks and any monitoring mechanisms, followed by navigating internal protections, which gives it a very low score. In contrast, the passenger carriage switch is merely hidden behind an overhead panel, which can be opened using basic tools. The attacker would still need understanding of the system and its vulnerabilities, and he would need to go undetected to perform the attack, justifying the medium score.

As for affected users, the driver’s cabin switch directly controls mission-critical functions, meaning that any successful attack can affect the entire train and safety systems, which gives it a very high score. For the passenger carriage switch, while its local role limits direct impact to one carriage, the interconnectivity with the critical switch increases its potential reach. As a result, its affected users score should be raised from low to very high, reflecting the possible system-wide consequences of compromise.

Regarding discoverability, both switches share similarities. The driver’s cabin switch is more physically protected, but identifying and understanding the vulnerabilities of either switch requires knowledge of their function, placement, and internal configuration. This level of insight demands technical reconnaissance and familiarity with the train’s internal systems. Thus, a low discoverability score is appropriate for both cases.

The overall DREAD analysis indicates that the driver’s cabin switch presents a lower risk, largely due to its physical protection and difficulty of exploitation. In contrast, the passenger carriage switch now represents a medium to high risk, not only because of its physical exposure and easier reproducibility, but also due to its potential as a stepping stone to compromise the critical switch in the driver’s cabin.

Man-in-the-Middle (MitM) attacks on service terminals involve intercepting and potentially modifying traffic between service terminals and the switches. Two scenarios are considered: one targeting the Control and Signalling terminal, which handles critical commands for train operations, and another targeting the CCTV terminal, responsible for surveillance data.

The following DREAD analysis in Table 4.17 evaluates the risk posed by a MitM attack on the Control and Signalling terminal.

Table 4.17 – Cyber-attack on the Control and Signalling terminal: MitM attack.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Very High	Very Low	Very Low	Very High	Low	Low

This analysis is very similar to the ones done before in tables Table 4.13 and Table 4.15. The damage potential is very high, as such attacks could directly impact train operations and safety. Reproducibility is very low, given the need to bypass VLAN security and access the driver’s cabin without getting noticed. Exploitability is also very low due to the security layers in place, while the affected users’ factor is very high due to the critical nature of the service. Discoverability is low, as identifying this vulnerability requires understanding the network architecture. This combination leads to a low-level risk.

For comparison purposes, the following DREAD analysis in Table 4.18 evaluates the risk posed by a MitM attack on the CCTV terminal on the passenger’s carriage.

Table 4.18 – Cyber-attack on the CCTV terminal: MitM attack.

	Dmg Pot	Reprod	Exploit	Aff User	Disc	Risk
Score	Very High	Medium	Low	Very High	Low	Medium-High

Initially, the damage potential would be considered as low, as compromising CCTV footage directly impacts security monitoring but does not influence train control systems. However, there is an additional risk if the attacker can send malicious video packets disguised as legitimate CCTV messages. These packets could exploit vulnerabilities in the passenger switch and if the network lacks proper segmentation or filtering, the attacker could then reach the switch in the driver’s cabin. From there, further attacks could be launched against critical systems elevating the potential impact. As a result, the

damage potential is rated very high. Reproducibility is assessed as medium, due to the lack of physical protection for the terminal and the relative ease of accessing it unnoticed in a public carriage. Exploitability is rated low, as successfully executing the attack would not only require access to the terminal but also a deep understanding of the underlying communication protocols and known vulnerabilities in the connected switch. The number of affected users is very high, since the entire train would be affected if the attacker succeeds in compromising a more important component. Discoverability is low because the terminal is only hidden and not physically protected, but the attacker would still need to perform a deep reconnaissance of the system to find vulnerabilities in the compromised targets. Even though the exploit requires some system knowledge and planning, the possibility of pivoting from the CCTV terminal to critical components, combined with the lack of physical security, results in a medium to high overall risk.

4.5.6 Security Evaluation: Attacker’s Perspective

After the presented analysis for each component, this section shifts the viewpoint to that of a potential attacker. Rather than assessing threats purely in terms of system vulnerability, the focus here is on evaluating which attack scenarios would be the most attractive and feasible from an adversary’s perspective. This includes considering the attacker’s required skill level, the ease of execution, the potential gain in terms of financial damage to the operator, and the possible impact on the operator’s public reputation.

Table 4.19 – Attacker’s perspective: Base Station.

Attack	Risk	Attacker Type	Ease of Execution	Attacker’s Gain	Reputation Impact
Damage/Destruction of components	High	Both	Easy	High	Medium
Radio Jamming	Medium	Both	Medium	Medium	Medium
Bypassing Access Control	Low	High Skilled	Very Hard	Very High	Very High

From the attacker’s point of view, the base station presents a diverse range of opportunities, each with distinct motivations and trade-offs as depicted in Table 4.19. The destruction of components is particularly appealing due to its high impact and ease of execution, especially since it does not require deep technical knowledge, only physical access and opportunity. The resulting financial damage from equipment replacement and service disruption is substantial, although the reputational damage remains moderate, as such physical attacks are difficult to prevent entirely and are often viewed as acts of vandalism rather than security failures.

In contrast, bypassing the access control system is a far more sophisticated attack. While it is rated as low risk in practice due to its complexity and the multiple barriers involved, it carries the highest attacker gain and reputation impact. A successful compromise of this nature would imply complete security failure, undermining the operator’s credibility and raising public concern.

Radio jamming, sitting between these extremes, is a moderate-risk, moderately difficult attack that can cause temporary disruption without physical damage. It offers lower attacker gain but is still effective in causing delays and drawing attention to system weaknesses, thus resulting in a medium reputational impact.

Table 4.20 – Attacker’s perspective: Mobile Terminal.

Attack	Risk	Attacker Type	Ease of Execution	Attacker's Gain	Reputation Impact
Flooding with excessive connections	Medium	Both	Easy	Medium	Medium
Malware Injection	Low	High Skilled	Hard	Very High	Very High

The mobile terminal acts as the primary interface between the train and the 5G network, making it a highly strategic target. Among the threats evaluated, shown in Table 4.20, the flooding attack stands out due to its ease of execution and relatively low barrier to entry. It can disrupt communication with the control centre and trigger operational delays, which in turn leads to moderate financial loss. However, the reputational impact remains contained, as this type of disruption is typically perceived as a temporary technical issue rather than a systemic failure.

On the other hand, malware injection is significantly more dangerous despite being harder to execute. This attack requires deep technical expertise and access to internal systems, making it viable only for high-skilled adversaries. However, if successful, the attacker could take control of the mobile terminal, impersonate the control centre, and issue false commands to the train. This represents a severe escalation in both operational and safety impact, potentially leading to full train compromise. As a result, the attacker’s gain and reputation impact are both rated very high, making this one of the most critical threats despite its lower likelihood of execution.

Physical attacks on switches require minimal technical effort from the attacker, but the resulting impact varies depending on the component’s location. As shown in Table 4.21, damaging the switch located in the passenger carriage causes only limited disruption. Thanks to network redundancy, the train continues to operate normally, and the effect is confined to that specific carriage. This makes the attacker’s gain low and the reputational impact negligible, as passengers may not even perceive the issue.

Table 4.21 – Attacker’s perspective: Physical attack on switches.

Attack	Location	Risk	Attacker Type	Ease of Execution	Attacker's Gain	Reputation Impact
Damage/Destruction of switch	Passenger Carriage	Medium	Both	Easy	Low	Very Low
Damage/Destruction of switch	Driver's Cabin	Medium	Both	Easy-Medium	Medium	Medium

In contrast, damaging the switch in the driver’s cabin has a more visible effect. Although the system can

recover by switching control to the backup cabin, the process may lead to short delays and a temporary service interruption. This translates into a moderate attacker gain and a medium reputational impact, as visible delays can tarnish the company’s reliability from a public perception standpoint.

Table 4.22 – Attacker’s perspective: Cyber-attack on gateway servers.

Attack	Location	Risk	Attacker Type	Ease of Execution	Attacker's Gain	Reputation Impact
Traffic Injection	Passenger Carriage	Medium-High	High Skilled	Medium-Hard	Very High	Very High
Traffic Injection	Driver's Cabin	Low	High Skilled	Very Hard	Very High	Very High

Regarding cyber-attacks on gateway servers, Table 4.22 highlights these as some of the most attractive targets from the attacker’s perspective. These components are central to onboard communications, handling both critical and non-critical data flows. A successful traffic injection attack, whether on the passenger carriage or the driver’s cabin, would allow the attacker to intercept or forge communications within the system.

In both locations, the attacker’s gain and reputational impact are rated very high, since the consequences include potential compromise of vital train operations. The difference lies in the ease of execution: in the passenger carriage, weaker physical protection makes the attack moderately difficult, whereas in the driver’s cabin, stronger access restrictions make it very hard to execute, despite the outcome being equally severe if successful.

Table 4.23 – Attacker’s perspective: Cyber-attack on switches.

Attack	Location	Risk	Attacker Type	Ease of Execution	Attacker's Gain	Reputation Impact
Traffic Injection	Passenger Carriage	Medium-High	High Skilled	Medium	Very High	Very High
Traffic Injection	Driver's Cabin	Low	High Skilled	Very Hard	Very High	Very High

As presented in Table 4.23, switches are vital components of the train’s internal network, responsible for routing data between services and subsystems. A traffic injection attack on a switch, particularly in the passenger carriage, is relatively feasible, as these switches are only lightly concealed and lack strong physical protection. This makes the attack medium in execution difficulty, yet it offers very high attacker gain, since it can be used as a stepping stone to reach more critical components or inject false traffic into the network. The reputation impact is also very high, as a successful breach suggests the network was compromised through internal infrastructure.

In the driver’s cabin, executing the same attack becomes much more difficult, due to physical restrictions and enhanced security. However, the attacker gain, and reputation impact remain equally severe, as this switch may directly handle sensitive communication such as control and signalling. The feasibility may be lower, but the damage potential makes it a high-priority target for advanced threat actors.

Table 4.24 – Attacker’s perspective: Cyber-attack on service terminals.

Attack	Location	Risk	Attacker Type	Ease of Execution	Attacker's Gain	Reputation Impact
MitM (CCTV)	Passenger Carriage	Medium-High	High Skilled	Medium-Hard	Very High	Very High
MitM (Control and Signalling)	Driver's Cabin	Low	High Skilled	Very Hard	Very High	Very High

Service terminals offer attackers a unique opportunity to blend physical proximity with network-level attacks. As detailed in Table 4.24, performing a MitM attack on a CCTV terminal in the passenger carriage is moderately difficult but highly rewarding. These terminals are publicly accessible and only partially protected, meaning an attacker with sufficient technical skill could potentially intercept or manipulate data being transmitted. The attacker gain and reputational damage are both very high, especially if the attacker can pivot from the CCTV system to more sensitive services.

The same attack scenario in the driver’s cabin, targeting control and signalling terminals, is significantly more complex. The terminal is harder to access, making the ease of execution very low. Nonetheless, the potential impact of compromising such a terminal is catastrophic from both a safety and reputational perspective.

4.6 Risk Reduction

This section proposes countermeasures to mitigate the security risks identified in the previous analyses. It focuses on reducing the likelihood and impact of successful attacks against both the train and the base station components. Each proposed measure is evaluated in terms of its expected security benefit and the associated implementation costs.

4.6.1 Risk Reduction: Base Station

Securing the base station against physical destruction is crucial, even though it already has strong protective measures in place. The cabinet housing critical components is locked with a key, requiring both an authorised laptop and credentials to access the system. Additionally, an alarm is triggered whenever the cabinet is opened, providing immediate alerts to potential intrusions. While these measures already provide a solid defence, further enhancements could reduce the risk of physical sabotage. Reinforcing the cabinet with tamper-proof materials and shock-resistant enclosures would improve resistance against forced entry or impact damage. Strengthening perimeter security by adding motion sensors and CCTV cameras with real-time monitoring would allow faster detection of intrusion attempts. Integrating biometric authentication or electronic keycards instead of traditional keys would reduce the risk of unauthorised access due to lost or stolen keys.

However, in the railway scenario, where numerous base stations are spread across the country,

implementing these additional security measures at scale presents significant cost concerns. While the proposed upgrades would improve physical security, the existing protections already provide a strong deterrent against unauthorised access. The cost of reinforcing cabinets across all locations, installing widespread surveillance systems, and transitioning to biometric authentication would be substantial. Additionally, maintaining and monitoring these additional security measures would require continuous operational expenses. In this context, the current security measures are sufficient, and additional enhancements would not be cost-effective given the distributed nature of railway base stations.

4.6.2 Risk Reduction: Train

The security analysis of the train's internal components highlights vulnerabilities stemming from both physical and cyber threats. The only physical protection currently in place is that the driver's cabin is locked with a key, which can still be forcibly opened, leaving critical components inside the train susceptible to attacks. To mitigate these risks and improve resilience, several security enhancements are proposed.

One major concern is the absence of any physical intrusion detection system inside the train's compartments. To address this, it is proposed to install an alarm system with motion detection sensors inside the compartments housing critical components. These sensors would trigger an immediate alert to the Control Centre if unauthorised access were detected. The installation of motion detection alarms would provide immediate detection and response to intrusions, limiting the time window available for an attacker to compromise critical systems. The cost associated with this measure is relatively low per compartment, although there would be operational expenses related to real-time monitoring of alarms and the management of potential false positives.

To address the risk of malicious traffic originating from compromised components, an additional message inspection barrier should be introduced. This component, shown as a Firewall in Figure 4.12, would act as a filtering mechanism, analysing data coming from switches in the passenger's carriages before it reaches critical systems in the driver's cabin. A key example is the CCTV terminal, which could be compromised to send fake video messages. The inspection barrier would analyse video messages and detect anomalies by comparing them to previously sent data. Since CCTV footage from fixed cameras is expected to have consistent content over time, sudden drastic changes or manipulated frames could be flagged and deleted before reaching the driver's cabin. This new component could be added to the driver's cabin, just after the switch, meaning that any communication arriving would be filtered and analysed. With the addition of a new component, a new security evaluation would be needed. Since this component is inside the driver's cabin, the evaluation would be similar to the ones done in sections 4.5.4 and 4.5.5. Developing and deploying a message inspection system requires specialised software and hardware capable of analysing network traffic in real-time. It must be tuned to detect anomalies without causing excessive delays in data transmission. Given the diversity of services onboard (CCTV, emergency communications, etc.), the system must be adaptable and scalable. The cost includes installation, maintenance, and ongoing updates to keep up with evolving threats. Overall, this is a medium to high-cost improvement with a high security benefit.

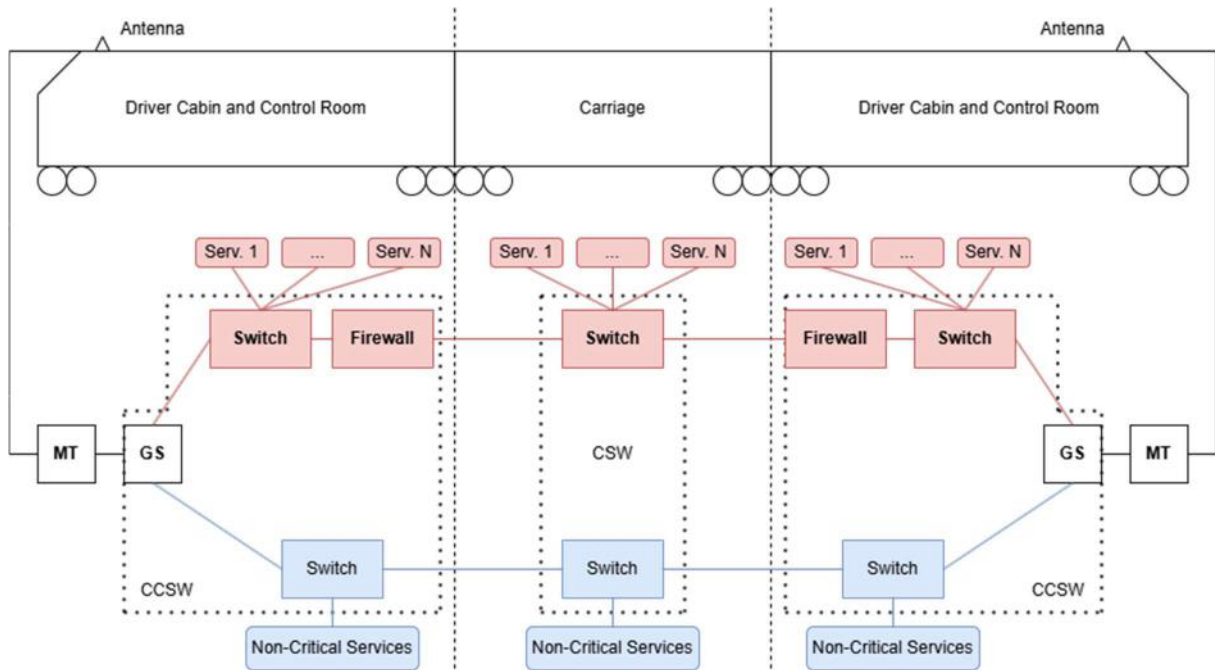


Figure 4.12 – Filtering component to prevent malicious packets arriving at the driver's cabin.

Furthermore, the current train network lacks encryption at the IP layer, leaving internal communications vulnerable to interception and tampering. To mitigate this, the adoption of IPsec is recommended, securing communications between all critical onboard components. IPsec would ensure that the data exchanged across the train's internal network is encrypted and authenticated, providing protection against both eavesdropping and unauthorised data modification. Nevertheless, this measure would involve moderate to high costs. These costs would stem from the need to upgrade the software or firmware of network devices, the potential requirement for more powerful hardware to handle encryption overhead, and the increased complexity in network management and key distribution.

In addition to these targeted countermeasures, architectural decisions also play a significant role in risk mitigation. As discussed in Section 3.4.3, the alternative architecture based on logical segregation introduces considerable security risks, as shown by Table 4.14. While it logically separates traffic streams, it greatly increases the number of critical components exposed to potential attacks. Each gateway server acts as an additional point of vulnerability that must be individually secured and monitored. The increased complexity not only raises the likelihood of configuration errors but also provides attackers with more opportunities to find and exploit weaknesses. For this reason, a key risk reduction measure is to avoid the implementation of this distributed gateway server architecture. Preferring the architecture based on physical segregation, where possible, simplifies the network, reduces the number of critical nodes, and makes it easier to defend and monitor. This decision would not generate additional costs; in fact, it could result in a cost saving by reducing the amount of hardware and maintenance required.

Chapter 5

Conclusions

This chapter finalises this work, summarising conclusions and pointing out aspects to be developed in future work.

This thesis focused on analysing the security of railway communication systems operating over 5G networks. The main goal was to identify both cyber and physical vulnerabilities and propose mitigation strategies. The study aimed to understand how modern cybersecurity risks affect complex and safety-critical railway systems, and to build a structured method for assessing risks and improving security.

The work began by describing the architecture of the railway communication network, covering its main components, including the control centre, base station, and onboard train systems. This provided the necessary context to understand which assets and services are critical and where the main vulnerabilities might exist. Two different train architectures were also presented: one based on physical segregation of critical and non-critical services, and another based on logical segregation using distributed gateway servers. These two architectures were later compared from a security perspective to assess their impact on the overall risk level. After the architectural analysis, a two-step methodology was followed: threats were first identified using the STRIDE framework, and their risk levels were then evaluated quantitatively using the DREAD model.

The security evaluation followed a structured and layered methodology designed to capture both physical and cyber vulnerabilities across the railway communication network. The analysis adopted a top-down approach, beginning at the Base Station, considered the highest point of failure impact, and then moving down to the train's internal components. This ensured that vulnerabilities with the potential to affect multiple systems were addressed first.

For the physical security analysis, components were grouped by their access pathways. All equipment inside the Driver's Cabin was assessed together, as access requires breaching a protected control room. Similarly, components located across the Passenger Carriages were grouped together, reflecting the different physical security challenges they present.

For the cybersecurity analysis, components were instead grouped by logical function. Service Terminals were analysed as a group due to their role in providing user-facing functionalities. Switches were treated together, given their central role in data flow and network management. Gateway Servers were assessed separately, as they concentrate and segregate critical and non-critical communications, making them particularly attractive targets. The Mobile Terminal was analysed individually due to its unique position as the train's communication bridge with the external 5G network.

The assessment of each component followed a three-step process. First, a STRIDE table was created to classify the types of threats applicable to each system, with the Repudiation category excluded as it was deemed irrelevant in this context. Second, for each STRIDE threat, a Tree of Threats was developed to map realistic attack paths. Each attack possibility was colour-coded: grey for negligible risks, yellow for manageable risks requiring further evaluation, and red for threats with significant risk that demanded in-depth analysis. Finally, attack scenarios were described based on the trees, and selected scenarios were evaluated using the DREAD model to quantitatively estimate their risk.

In addition, a classification table for each DREAD category was used to ensure consistent and objective scoring, improving the overall reliability of the risk assessment.

5.1.1 Conclusions

Several important conclusions were drawn from the analysis:

The base station was identified as a critical node in the communication chain, mainly exposed to DoS attacks through radio jamming or physical destruction of its components. Thanks to 5G's strong security mechanisms, remote cyber-attacks like spoofing, packet injection, or full takeover were found to be extremely difficult without insider help or major network vulnerabilities. Although physically destroying the base station would cause serious operational disruption, the actual likelihood of a cyber compromise was considered very low. Consequently, the base station's overall cyber risk is low, while physical DoS remains a significant threat to service continuity.

The analysis of the train's internal network showed that physical accessibility plays a major role in the security level of each component. Systems located inside the driver's cabin, protected by a locked door, were found to have a lower risk of attack compared to components hidden inside passenger carriages, where access is much easier for a potential attacker.

From a cyber perspective, the Gateway Servers and onboard switches presented major risks. Gateway Servers, which manage the separation of critical and non-critical communications, were identified as attractive targets for traffic injection attacks. If compromised, an attacker could inject false control messages and interfere with train operations. Similarly, onboard switches, especially those inside the driver's cabin, control critical services like signalling and command functions, making them high-value targets. Attacks on these switches could cause serious service disruptions, operational delays, or even impact safety.

The analysis showed clear differences between attacking components located inside the driver's cabin and those placed in the passenger carriages. Systems inside the driver's cabin, such as the switches and gateway servers, benefit from stronger physical protections, making them harder to access. However, if an attacker succeeds in compromising these components, the consequences would be severe. Full or partial control over critical services like train control, signalling, and communications could be achieved, leading to very high financial losses and significant damage to the company's reputation.

In contrast, components located inside the passenger carriages, such as CCTV terminals, service gateways, and local switches, are much easier to physically access, due to weaker protection. Attacks against these elements are simpler to execute but generally have a lower direct impact. On their own, compromising these components would mostly result in the loss of auxiliary services, such as surveillance or passenger communication, without immediately affecting train operations. However, these components could still serve as pivot points, allowing an attacker to escalate privileges and target more critical systems later.

Overall, attacking components in the driver's cabin presents a higher risk in terms of financial damage and public image, despite being harder to achieve. Attacking components in the passenger carriage is easier but initially less impactful unless used as part of a broader, multi-stage attack.

Following the security assessment, several countermeasures were proposed to reduce the risks identified across the railway network. The risk reduction measures targeted both physical and cyber threats and were selected based on their expected security benefits relative to their implementation costs.

To strengthen physical security, it was proposed to install motion detection alarms inside the compartments housing critical components. This would allow faster detection of unauthorised access attempts, particularly for equipment located in passenger carriages. This measure offers a strong security improvement with a relatively low installation cost, although operational costs related to monitoring alarms would also need to be considered.

At the network level, the deployment of a message inspection barrier after the switches in the driver's cabin was recommended. This barrier would inspect traffic for anomalies or malicious messages before they reach critical systems such as control and signalling. This measure would significantly improve protection against traffic injection attacks originating from compromised components in the passenger carriages. However, it would involve medium to high costs, both in acquiring specialised hardware and integrating it into the train network securely.

To further protect data transmissions inside the train, the adoption of IPSec across the internal IP network was also proposed. Encrypting communications between onboard devices would mitigate risks such as man-in-the-middle attacks or unauthorised packet injections. While IPSec would provide strong security benefits, its implementation would require software upgrades, possible hardware reinforcements due to encryption overhead, and increased complexity in network management.

Finally, a critical architectural recommendation was made concerning the choice between physical and logical segregation of services. The alternative architecture based on logical segregation with multiple distributed gateway servers, although improving flexibility, was found to significantly increase the system's attack surface. Each additional gateway server would present a new point of vulnerability, complicating system protection. Therefore, it was concluded that physical segregation, where critical and non-critical traffic is kept separate through dedicated paths, provides a more secure and manageable solution, with no added cost compared to the more complex logical segregation design.

5.1.2 Limitations

While the security analysis presented in this thesis covers a wide range of threats and vulnerabilities, there are some limitations that should be acknowledged.

Firstly, the study focused exclusively on the 5G-based communication systems used by the train and did not consider the parallel onboard WiFi network. In practice, WiFi systems could present additional vulnerabilities, and potential interactions between WiFi and 5G networks might create new attack paths that were not analysed here.

Secondly, the analysis considered the separation between critical and non-critical services but did not investigate in detail whether non-critical services could be exploited to indirectly compromise critical services. Although the architectures assume logical or physical separation, advanced attackers could

attempt to pivot through less protected components to reach high-value targets. Including this type of lateral movement analysis would strengthen future evaluations.

Another limitation is related to the evolving nature of the FRMCS (Future Railway Mobile Communication System) standard. As FRMCS is still under development, some technical details or security mechanisms may change before final deployment. However, the methodology developed in this thesis, based on threat modelling with STRIDE, risk evaluation with DREAD, and component-by-component analysis, was designed to be adaptable. It can be updated and applied to future architectures with minimal adjustments once FRMCS specifications are finalised.

From a critical point of view, the analysis successfully highlighted the importance of physical protections, and the risk associated with internal network compromises. However, it relied on assumed attacker models and static component behaviour. Real-world systems often face dynamic threats, such as attackers who adapt strategies based on system responses. More dynamic threat simulation, including red-teaming exercises or attack emulation, would be valuable to further validate the findings.

5.1.3 Future Work

For future work, several directions are recommended. Expanding the analysis to include potential attack paths from non-critical to critical services would provide a more complete security assessment. Investigating the interaction between WiFi and 5G communications onboard the train would also be important, especially considering possible bridges between the two networks. Additionally, future studies could simulate active attack scenarios on testbed environments to validate theoretical risk assessments and refine mitigation strategies. As FRMCS evolves, repeating the threat analysis against the finalised standard would ensure that security strategies remain aligned with operational needs. Furthermore, the development of a simulator capable of emulating the entire railway network would be highly beneficial, as it would enable comprehensive testing of attack scenarios and countermeasures in a controlled and reproducible environment.

Annex A

4G Onboard Communication System

This annex presents the 4G Onboard Communication System used by HITACHI in some of Chile's trains.

(confidential information)

Figure A.6.1 – Onboard communication system's topology used by HITACHI in Chile's trains.

References

- [1] Check Point, “2023 Cyber Security Report.” Accessed: Feb. 07, 2024. [Online]. Available: <https://pages.checkpoint.com/cyber-security-report-2023.html>
- [2] John Leyden, “Polish teen derails tram after hacking train network.” Accessed: Jan. 15, 2025. [Online]. Available: https://www.theregister.com/2008/01/11/tram_hack/
- [3] The Guardian, “‘Cyber-attack’ hits Iran’s transport ministry and railways.” Accessed: Apr. 18, 2025. [Online]. Available: <https://www.theguardian.com/world/2021/jul/11/cyber-attack-hitsirans-transport-ministry-and-railways>
- [4] UIC, “The worldwide professional association representing the railway sector and promoting railway transport” Accessed: Nov. 25, 2023. [Online]. Available: <https://uic.org/about/about-uic/>
- [5] RailEngineer, “The future of GSM-R?” Accessed: Nov. 20, 2023. [Online]. Available: <https://www.railengineer.co.uk/the-future-of-gsm-r/>
- [6] UIC, “FRMCS: FUTURE RAILWAY MOBILE COMMUNICATION SYSTEM.” Accessed: Mar. 20, 2023. [Online]. Available: <https://uic.org/rail-system/telecoms-signalling/frmcs>
- [7] 5GRAIL, “5GRAIL.” Accessed: Nov. 22, 2023. [Online]. Available: <https://5grail.eu/>
- [8] J. Eberspächer, H.-J. Vögel, C. Bettstetter, and C. Hartmann, GSM - Architecture, Protocols and Services, 3rd ed. 2008, ISBN 978-0-470-03070-7
- [9] W. Gheth, K. M. Rabie, B. Adebisi, M. Ijaz, and G. Harris, “Communication systems of highspeed railway: A survey,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, Apr. 2021, doi: 10.1002/ett.4189.
- [10] A. Sniady and J. Soler, “An overview of GSM-R technology and its shortcomings.,” 12th International Conference on ITS Telecommunications, pp. 626–629, 2012.
- [11] ETSI, “Rail Communications (RT).” Accessed: Nov. 24, 2023. [Online]. Available: <https://www.etsi.org/technologies/rail-communications>
- [12] ETSI, “Railways Telecommunications (RT); Global System for Mobile communications (GSM); Detailed requirements for GSM operation on Railways,” 2004. [Online]. Available: http://portal.etsi.org/chaircor/ETSI_support.asp
- [13] ETSI, “Railways Telecommunications (RT); Global System for Mobile communications (GSM); Detailed requirements for GSM operation on Railways,” 2006. [Online]. Available: http://portal.etsi.org/chaircor/ETSI_support.asp
- [14] ETSI, “European Standard (Telecommunications series) Global System for Mobile

- communication (GSM); Requirements for GSM operation on railways,” 2005. [Online]. Available: http://portal.etsi.org/chaircor/ETSI_support.asp
- [15] European Commission, “ETCS Levels and Modes.” Accessed: Feb. 10, 2023. [Online]. Available: https://transport.ec.europa.eu/transport-modes/rail/ertms/what-ertms-and-how-does-itwork/etcs-levels-and-modes_en
- [16] Z. Yu, H. Wang, and F. Chen, “Security of railway control systems: A survey, research issues and challenges,” *High-speed Railway*, vol. 1, no. 1, pp. 6–17, Mar. 2023, doi: 10.1016/j.hspr.2022.12.001.
- [17] 3GPP, “5G System Overview.” Accessed: Dec. 05, 2023. [Online]. Available: <https://www.3gpp.org/technologies/5g-system-overview>
- [18] ETSI, “TS 123 501 - V17.4.0 - 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 17.4.0 Release 17),” 2022. [Online]. Available: <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>
- [19] S. Zhang, “An Overview of Network Slicing for 5G,” *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, Jun. 2019.
- [20] NGMN, “Page 1 (7) NGMN 5G Project Requirements & Architecture-Work Stream E2E Architecture Version NGMN 5G P1 Requirements & Architecture Work Stream End-to-End Architecture Description of Network Slicing Concept by Next Generation Mobile Networks Alliance,” 2016.
- [21] Kutub Thakur and Al-Sakib Khan Pathan, *Cybersecurity Fundamentals: A Real-World Perspective*. CRC Press/Taylor & Francis Group, 2020, eBook ISBN 9781003035626.
- [22] Rajesh Kumar Goutam, *Cybersecurity Fundamentals: Understand the Role of Cybersecurity, Its Importance and Modern Techniques Used by Cybersecurity Professionals*. BPB Publications, 2021, ISBN-10 9390684730.
- [23] G. J. Popek and C. S. Kline, “Encryption and Secure Computer Networks,” *ACM Computing Surveys (CSUR)*, vol. 11, no. 4, pp. 331–356, 1979.
- [24] A. Y. A. Al-Tamimi, M. A. Snober, and Q. A. Al-Haija, “A Performance Evaluation Study to Optimize Encryption as a Service (EaaS),” in *Lecture Notes in Electrical Engineering*, Springer Science and Business Media Deutschland GmbH, 2023, pp. 681–691. doi: 10.1007/978-981-19-7753-4_52.
- [25] H. Wu, “The Hash Function JH,” NIST (Round 3), 2011.
- [26] Asmaa Shaker Ashoor and Prof. Sharad Gore, “Importance of Intrusion Detection System (IDS),” *International Journal of Modern Communication Technologies & Research (IJMCTR)* ISSN: 2321-0850, 2010.
- [27] Wentz Wu, “Extensible Authentication Protocol (EAP).” Accessed: Jan. 07, 2024. [Online]. Available: <https://wentzwu.com/2020/03/04/extensible-authentication-protocol-eap/>

- [28] W. Xiong and R. Lagerström, "Threat modeling – A systematic literature review," *Computers & Security*, vol. 84, pp. 53-69 Jul. 01, 2019, *Elsevier Ltd*.
- [29] D. A. Frincke and M. Bishop, "About Penetration Testing," 2007. [Online]. Available: 89 www.computer.org/security/
- [30] S. Hussain, S. Iqbal, A. Kamal, S. Ahmad, and G. Rasool, "Threat Modelling Methodologies: A Survey," *Sci.Int.(Lahore)*, vol. 26, no. 4, pp. 1607–1609, 2014, [Online]. Available: <https://www.researchgate.net/publication/307902746>
- [31] SoftwareSecured, "Comparison of STRIDE, DREAD & PASTA." Accessed: Dec. 15, 2023. [Online]. Available: <https://www.softwaresecured.com/post/comparison-of-stride-dreadpasta#stride-2>
- [32] S. M. Bellovin and W. R. Cheswick, "Network firewalls," in *IEEE Communications Magazine*, vol. 32, no. 9, pp. 50-57, Sept. 1994, doi: 10.1109/35.312843.
- [33] R. Venkateswaran, "Virtual private networks," *IEEE Potentials*, vol. 20, no. 1, pp. 11–15, 2001.
- [34] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, "Guide to IPsec VPNs," Special Publication (NIST SP) - 800-77 Rev 1, Gaithersburg, MD, Jun. 2020. doi: 10.6028/NIST.SP.800-77r1.
- [35] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. Van Der Merwe, "A comprehensive symbolic analysis of TLS 1.3," in *Proceedings of the ACM Conference on Computer and Communications Security*, Association for Computing Machinery, Oct. 2017, pp. 1773–1788. doi: 10.1145/3133956.3134063.
- [36] X. Huang, T. Yoshizawa, and S. B. M. Baskaran, "Authentication mechanisms in the 5G system," *Journal of ICT Standardisation*, vol. 9, no. 2, pp. 61–78, 2021, doi: 10.13052/jicts2245-800X.921.
- [37] Y. Xiao and Y. Wu, "5G-IPAKA: An Improved Primary Authentication and Key Agreement Protocol for 5G Networks," *Information (Switzerland)*, vol. 13, no. 3, Mar. 2022, doi: 10.3390/info13030125.
- [38] A. R. Prasad, S. Arumugam, S. B, and A. Zugenmaier, "3GPP 5G Security," *Journal of ICT Standardisation*, vol. 6, no. 1, pp. 137–158, 2018, doi: 10.13052/jicts2245-800X.619.
- [39] F. Salahdine, T. Han, and N. Zhang, "Security in 5G and beyond recent advances and future challenges," *Security and Privacy*, vol. 6, no. 1, Jan. 2023, doi: 10.1002/spy2.271.
- [40] F. Kandah, Y. Singh, and W. Zhang, "Mitigating eavesdropping attack using secure key management scheme in wireless mesh networks," *Journal of Communications*, vol. 7, no. SPL.ISS. 8, pp. 596–605, 2012, doi: 10.4304/jcm.7.8.596-605.
- [41] L. Correia, "Mobile Communication Systems," *Lecture Notes*, Instituto Superior Técnico, University of Lisbon, Lisbon, Portugal, Feb. 2020.
- [42] "Recommendation ITU-R M.2083-0 IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond M Series Mobile, radiodetermination, amateur and

- related satellite services,” 2015. [Online]. Available: <http://www.itu.int/ITU-R/go/patents/en>
- [43] European Integrated Railway Radio Enhanced Network, “Functional Requirements Specification Version 8.0.0,” 2015.
- [44] N. Henrique Vicente da Silva, L. Manuel De Jesus Sousa Correia, and J. Eduardo Charters Ribeiro da Cunha Sanguino Supervisor, “Evaluation of Train Communications Interference-Free Regions along Rail Tracks Electrical and Computer Engineering Examination Committee,” Instituto Superior Técnico, University of Lisbon, Lisbon, Oct 2020.
- [45] ETSI, “TS 122 289 - V16.1.0 - LTE; 5G; Mobile communication system for railways (3GPP TS 22.289 version 16.1.0 Release 16),” 2020. [Online]. Available: <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>
- [46] S. Soderi, D. Masti, and Y. Z. Lun, “Railway Cyber-Security in the Era of Interconnected Systems: A Survey,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 6764–6779, Jul. 2023, doi: 10.1109/TITS.2023.3254442
- [47] Zhao, Hui & Dai, Xuewu & Ding, Lei & Cui, Dongliang & Ding, J.L. & Chai, Tianyou. (2021). Resilient Cooperative Control for High-Speed Trains Under Denial-of-Service Attacks. *IEEE Transactions on Vehicular Technology*. 70. 12427-12436. 10.1109/TVT.2021.3120695.
- [48] M. Heddebaut et al., “Towards a resilient railway communication network against electromagnetic attacks,” France, Apr. 2014. [Online]. Available: <https://hal.science/hal01061258>
- [49] H. Pirayesh and H. Zeng, “Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey,” 2022, Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/COMST.2022.3159185.
- [50] Thales, “5G-based Communications for Railway Operations.” Accessed: Dec. 13, 2023. [Online]. Available: <https://www.thalesgroup.com/en/5g-based-communications-railway-operations>
- [51] Thales, “Welcome to the 5G Railway.” Accessed: Dec. 13, 2023. [Online]. Available: <https://www.thalesgroup.com/en/worldwide/transport/magazine/welcome-5g-railway>
- [52] UIC, “FRMCS Specifications.” Accessed: Dec. 13, 2023. [Online]. Available: <https://uic.org/railsystem/telecoms-signalling/frmcs#FRMCS-Specifications>
- [53] R. He et al., “5G for Railways: Next Generation Railway Dedicated Communications,” *IEEE Communications Magazine*, vol. 60, no. 12, pp. 130–136, Dec. 2022, doi: 10.1109/MCOM.005.2200328.
- [54] Ana Gonzalez-Plaza, Juan Moreno, Iñaki Val, Aitor Arriola, and Pedro M Rodriguez, “5G Communications in High Speed and Metropolitan Railways,” 2017.
- [55] A. H. Carlson, D. Frincke, and M. J. Laude, “Railway Security Issues: A Survey of Developing Railway Technology.”
- [56] M. Kiviharju, S. Rikkonen, C. Lassfolk, and H. Kari, “A Cryptographic and Key Management Glance at Cybersecurity Challenges of the Future European Railway System,” 2022.

- [57] M. N. I. Farooqui, J. Arshad, and M. M. Khan, "A Layered Approach to Threat Modeling for 5G-Based Systems," *Electronics* 11, no. 12: 1819, Jun. 01, 2022, MDPI. <https://doi.org/10.3390/electronics11121819>
- [58] B. Santos et al., "Threat Modelling for 5G networks," in 2022 International Wireless Communications and Mobile Computing, IWCMC 2022, Institute of Electrical and Electronics 91 Engineers Inc., 2022, pp. 611–616. doi: 10.1109/IWCMC55113.2022.9825149.