Cybersecurity and Risk Management in Implementing Future Railway Mobile Communications System

Samuli Korpimäki

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.
Espoo 6.12.2023

Supervisor

Prof. Jukka Manner

Advisor

MSc Tomi Lankinen

Aalto University
School of Electrical
Engineering

Aalto University
School of Electrical
Engineering

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi
Abstract of the master's thesis

Author Samuli Korpimäki

Title Cybersecurity and Risk Management in Implementing Future Railway Mobile Communications System

Degree programme Computer, Communication and Information Sciences

Major Communications Engineering **Code of major** ELEC3029

Supervisor Prof. Jukka Manner

Advisor MSc Tomi Lankinen

Date 6.12.2023 **Number of pages** 68 **Language** English

Abstract

This thesis looked at the cybersecurity risks that rise from moving to a wireless communication system. The goal was to identify risks related to Future Railway Mobile Communication System and European Train Control System. The identified risks were then evaluated by the railway cybersecurity technical specification CLC/TS 50701. The methods used in this process were literature surveys, expert interviews and initial risk assessment described in CLC/TS 50701. As the results of the risk analysis we noticed that most of the risks are mitigated by current cybersecurity and safety standards.

Keywords FRMCS, ETCS, ERTMS, risk assessment, CLC/TS 50701, cybersecurity, railways

Aalto University
School of Electrical
Engineering

Aalto-yliopisto, PL 11000, 00076 AALTO
www.aalto.fi
Diplomityön tiivistelmä

Tekijä Samuli Korpimäki

Työn nimi Kyberturvallisuus ja riskien hallinta uuteen rautatiekommunikaatiojärjestelmään siirryttäessä

Koulutusohjelma Elektroniikka ja sähkötekniikka

Pääaine Tietoliikennetekniikka **Pääaineen koodi** ELEC3029

Työn valvoja Prof. Jukka Manner

Työn ohjaaja MSc Tomi Lankinen

Päivämäärä 6.12.2023 **Sivumäärä** 68 **Kieli** Englanti

Tiivistelmä

Tässä työssä katsottiin kyberturvallisuus riskejä, jotka nousevat langattomaan tiedonsiirtojärjestelmään siirryttäessä. Tavoitteena oli tunnistaa riskejä jotka liittyvät tulevaisuuden rautatiemobiilikommunikaatiojärjestelmään ja Eurooppalaiseen junakulunvalvontajärjestelmään. Tunnistetut riskit arvioitiin rautateiden kyberturvallisuus määritelmän CLC/TS 50701 mukaan. Työn suorittamiseen käytettiin kirjallisuuskatsausta, asiantuntijahaastatteluita ja CLC/TS 50701:ssä esitettyä alustavaa riskienhallintaa. Tuloksissa huomattiin että uusia riskejä voidaan pienentää käyttämällä jo olemassa olevia kyberturvallisuus ja turvallisuus standardeja.

Avainsanat FRMCS, ETCS, ERTMS, riskien arviointi, CLC/TS 50701, kyberturvallisuus, rautatiet

Preface

I would like to thank my professor Jukka Manner for the good discussions and feedback for this thesis. A special thanks also goes to Eeva Halonen for supporting me in the thesis process. A thank you also goes to my family for being understanding and supporting me during my studies.

Otaniemi, 6.12.2023

Samuli O. Korpimäki

Contents

Symbols and abbreviations

Abbreviations

AES	Advanced Encryption Standard
ATP	Automatic Train Protection
APT	Advanced Persistent Threat
DES	Data Encryption Algorithm
DMI	Driver Machine Interface
EMI	Electromagnetic Interference
ENISA	European Union Agency for Cybersecurity
EDP	European Deployment Plan
ERA	European Railway Agency
ERTMS	European Railway Traffic Management System
ETCS	European Train Control System
FTIA	Finnish Transport Infrastructure Agency
FRMCS	Future Railway Mobile Communication System
GSM-R	Global System for Mobile communications - Railway
IT	Information Technology
IXL	Interlocking
IEC	International Electrotechnical Commission
JKV	Junakulunvalvonta (Finnish national train control)
KMS	Key Management System
MCx	Mission Critical service
MNO	Mobile Network Operator
NTC	National Train Control
OBU	On-Board Unit
OT	Operational Technology
QoS	Quality of Service
RBC	Radio Block Centre
STM	Specific Transmission Module
SuC	System under Consideration
3DES	Triple Data Encryption Algorithm
3GPP	3rd Generation Partnership Project
UE	User Equipment

1 Introduction

Railway transportation is an important piece of everyday commuting and hauling of goods. Just in Europe it was estimated to have generated 416 billion passenger kilometers in 2019, which is a 3.4% increase from 2018[1]. Due to COVID-19, this increase stopped in 2020 and there was a sharp decline in passenger kilometers. However even during 2020 the transport of goods maintained levels closer to 2019 [3]. As the trend was growing before the pandemic, it can be expected that the numbers will return to previous levels in the near future.

In order to ensure the safety of these passengers and freight, Europe has been moving towards the European Railway Traffic Management System (ERTMS) and European Train Control system (ETCS). The base of these systems comes from the European Council directive 96/48/EC[2], which started the regulation towards an unified European railway. The aim of these systems is to achieve seamless traffic by rail across country borders and to ensure the same standards of safety and operation.

The ERTMS/ETCS system is divided into levels of operation based on the underlying technology used. There are three base levels and two added levels. Level 0 represents a railway line not equipped with ETCS. Level Special Transmission Module (STM) is for a national train management system that is not ETCS.[4] Level 1 uses balises, which can be thought of as giant RFID tags, to achieve point based communication of track information with the train while driver-controller communications are done by radio. Level 2 ETCS uses wireless communications systems to transmit the data between the train and track side systems. In level 2 the balises are still kept in use to calibrate the odometer and keep location data accurate. Level 3 is based on level 2, but introduces new concepts such as train integrity checks and moving safety zones around trains. This increases traffic capacity as trains can operate closer to each other. Level 2 and 3 also make trackside signals optional.[5]

GSM-R has been in use for the ETCS communications in level 1 (voice) and 2. GSM-R has been successful and has been widely adopted even outside of Europe covering 400,000 km of tracks worldwide [7]. However as the name suggests, GSM-R is a modified Global System for Mobile communications (GSM) system. This 2G+ system cannot fulfill the increasing needs of ETCS level 2 and 3 communications and has been predicted to be obsolete by 2030. This has lead to the search of a replacement system which has been named as Future Railway Mobile Communications System (FRMCS).

The Future Railway Mobile Communications System is expected to enable key services for the railway industry in the future. These services include real-time video surveillance, train-to-train direct communications, train multimedia dispatching, railway internet of things (RIoT) and internet access on high-speed trains.[11] Outside of the internet access, the services are directed towards safety and increasing capacity, which are key values in railway business. The internet access is also an important issue, as even in low speed situations the train carriage increases attenuation of mobile signals[13].

5G technology has been widely considered as the new FRMCS base. The International Union of Railways (UIC) has worked with 3rd Generation Partnership

Program (3GPP) to include railway use cases in 3GPP Release 16 and 17. This makes for a strong argument for using 5G, however the current use cases for FRMCS are network agnostic so any network that fulfills the requirements can be used, such as LTE-Advanced (also known as 4.9G)[8].

Finland is currently moving towards ETCS level 2 implementation[9]. At the moment Finland is using ETCS level 1 and a national train control system through Specific Transmission Module (STM). The Digirail-project aims to do a complete upgrade of railway command, control and signalling systems in Finland. There is currently no GSM-R network in Finland, therefore one important goal of this upgrade is to skip over GSM-R straight to a 5G FRMCS network. This upgrade has already started in Finland between Kouvola, Kotka and Hamina (KoKoHa), which includes the busiest freight track of Finland.

Railway operational technology has long been isolated as a wired system. Therefore moving towards a wireless control system opens it up to different threats compared to before. To date cyber attacks have been mostly targeted towards the IT side of railways, such as ticketing systems[10]. These attacks of course inconvenience users due to trains getting delayed or cancelled, however they do not pose a threat as significant as losing control of a train. Railway operational technology has so far only been the target of relatively few attacks[10], but with the rise of automation and easier access through wireless technologies more attacks are to be expected.

Cybersecurity is becoming an increasingly important part of running any business, moreover in a critical system such as transportation. EU has taken note of this and in 2020 published a toolkit for 5G cybersecurity[12]. The toolkit offers ways to mitigate main risks of 5G networks. One of the main things in cybersecurity is to continually observe possible threats to keep up with the development of attack vectors and technology. A method that can be used for this is risk analysis.

Cybersecurity risks can not be managed in the exact same way as safety risks or hazards. While safety risks are usually analysed by their frequency and impact, there is no real frequency or chance inherent to cybersecurity risks. We can not know when someone decides to hack or interfere with our system, therefore security risks are more about vulnerabilities and exposure. Due to this, security risks are also always changing. Risk management for security needs to be updated constantly to keep track of new threats.

The goal of this thesis is to update the ERTMS/ETCS risk analysis to include the move to ERTMS/ETCS level 2 in Finland. This thesis will be done as part of the Digirail-project in Finland and will be related to the KoKoHa test track. The main questions that this thesis aims to answer are:

- What are the new cybersecurity risks in 5G related to ERTMS/ETCS level 2?
- How can these risks be mitigated based on current standards?
- What do these new FRMCS related risks mean for the railway systems?

As part of these questions we will have a short look at what Mission Critical Service (MCX) brings to the railway sector. MCX is a critical piece of the communication system that will be between the train and trackside applications. As such special interest to this thesis subject is what kind of end-to-end security does the MCX offer.

The thesis subject will be limited to the ERTMS/ETCS system as a whole, and will not go into detail regarding block level interactions. The risk analysis focus will also be in the level 2 implementation and cybersecurity, although some parts from lower levels are necessary. The thesis will also be limited to the 5G test lab planned in the Digirail-project.

The thesis is divided to four parts. In the first part the railway systems in use, such as ERTMS/ETCS and railway communication systems, are introduced. In the second part the relevant railway safety standards, cybersecurity and risk analysis are looked at. The third part shows the results of this thesis and the final part will conclude the thesis.

The methods used in this thesis will be literature survey, expert interviews and expert workshops. The background part of the thesis will be done as a literature survey. The risk analysis will be based on the expert interviews and workshops, and will be done in a qualitative way, as security risks can't be easily analysed by quantitative methods. The methods for the risk analysis are described more in Section 3.4 and in the results.

2 Modern railway systems

In this chapter we will introduce the railway systems currently in use in Europe and more specifically Finland. We go over the basics of how these systems work and why they are in use. The railway communication systems that are currently in use and what is planned for the future will also be looked at.

During this thesis there were two persons interviewed. These were used to gain background knowledge on key aspects of railway system needed in this thesis. The experts interviewed were:

- Peteveikko Lyly from FTIA. Several interviews relating to the FRMCS specification and the FTIAs opinion on them.
- Thomas Raschke from Eisenbahn-Bundesamt (Federal Railway Authority of Germany). A phone interview regarding the ETCS level 2 and risk management.

Other interviews were planned at the beginning of the thesis, but they were not conducted due to the project behind this thesis being changed while the thesis was still being developed. While the focus moved slightly away from expert interviews, the participants time and effort is greatly appreciated.

2.1 Traffic management and train control systems

This section is focused on the European Railway Traffic Management System (ERTMS) and European Train Control System (ETCS). The ERTMS system and different levels of ETCS operation will be introduced in subsection 2.1.1. The status of these systems and the train control system currently in use in Finland will be described in subsection 2.1.2.

Technical terms needed in this section:

- **Balise** is a physical short range radio device located between the tracks. A train will pass over the balise and read the information with a reader device. The concept is similar to RFID.
- **Eurobalise** is a balise used with European standards as part of ERTMS/ETCS.
- **Interlocking** is a system used for making sure that only one train has physically possible access to a part of a track.
- **Movement authority** is information given to the train that tells the train, that it is safe to move up to a certain point. A train that has no movement authority will have to stop and wait until it is granted.
- **Euroloop** is a loop computer used to achieve semi-continuous communication with a train. It is comprised of a long wire used to send signals and a control chip.
- **Lineside electronic unit** generates the messages that the balises send based on track information available.

2.1.1 European systems

Europe started the process of creating an unified railway traffic management system in 1996 by publishing the directive 96/48/EC . This directive created the base for

the ERTMS and ETCS systems.[2] However large scale implementation has only recently started. One reason for this is that railways have a long expected use time of several decades. In early 2017 European commission implemented regulation 2017/6 [14] which set up the expected implementation times of ERTMS systems in the core railway networks. This planned implementation is called the ERTMS European Deployment Plan (EDP).

According to the European ERTMS Coordinators work plan [15], in May 2020 12% (6 120,54 km) of the core network corridors were using ETCS. This was about 78% of the EDP target for the end of 2019. The plan sets the target of 15 682 km tracks with ETCS by 2023.

The ERTMS at present consists of two components, ETCS and GSM-R. ETCS is responsible for the supervision of train movements, such as current speed, and driver actions. If non-permitted activity is detected, for example going over the speed limit, the ETCS can take over the control of the train and activate the brakes. GSM-R is used as the communications medium between the train, traffic control and trackside equipment.[5]

There are currently five levels defined for ERTMS/ETCS operation, which are levels 0-3 and National Train Control (NTC). While these levels have different communication types between the train and trackside, this communication is critical to train operation. This communication can provide movement authority and different track conditions to help the driver and the system to operate the train safely.

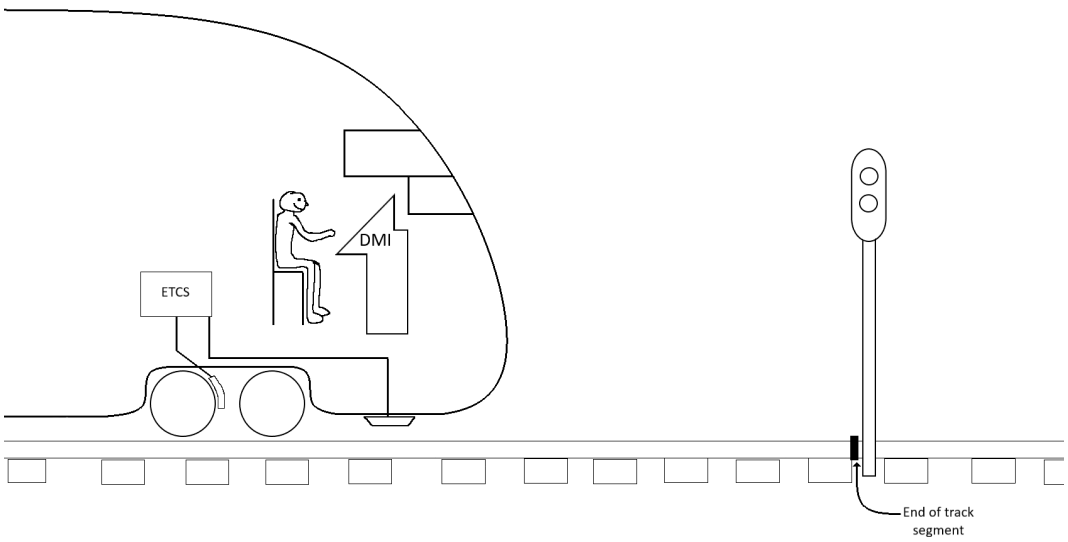

Figure 1: ERTMS/ETCS level 0

Level 0: Operation on level 0 depends on having optical trackside signals to

be able to convey movement authority to the driver. Level 0 covers lines that are not fitted with ERTMS or a national train control system. In cases of trackside equipment failures it is also possible to fall to level 0 due to the control system being inaccessible. ETCS equipped trains can be run on level 0 tracks, but the on-board ERTMS equipment provides no supervision outside of the maximum specified speed of the train type in unfitted areas. The only information change between the track and the train happens when a level transition needs to happen.[5]

Level NTC: In level NTC the train is equipped with both ETCS and a NTC system. The NTC can be connected to the ETCS through a Specific Transmission Module (STM) to allow management of the national system. STM needs to be in use for a NTC to be able to access on-board ETCS equipment such as the driver machine interface (DMI). The capabilities of operation on level NTC are based on the underlying national system. Sharing resemblance with level 0, level NTC doesn't use ETCS train-track communication outside of level transitions.[5]

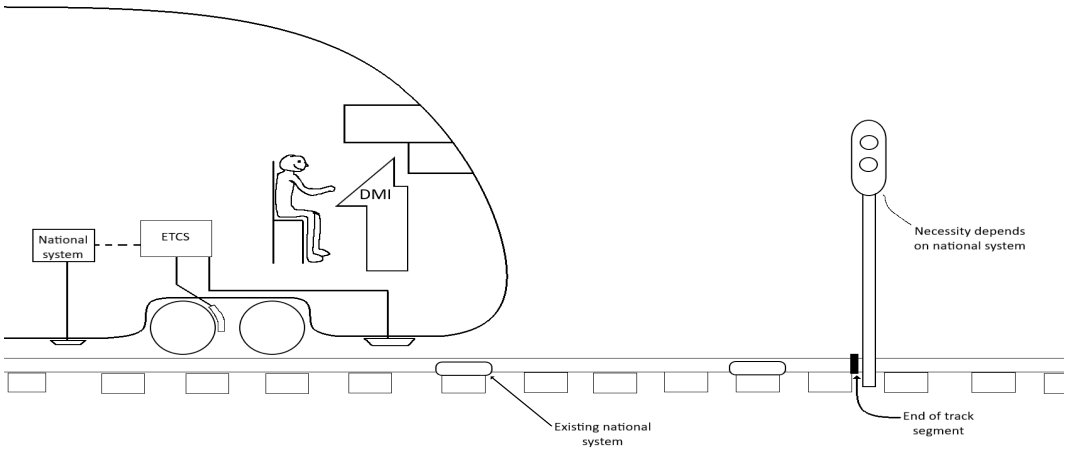

Figure 2: ERTMS/ETCS level NTC

Level 1: Level 1 systems are based on Eurobalises that enables spot transmission between the train and trackside equipment. The trackside systems are responsible for detecting the location of the train and the integrity of the train. When the trackside systems have deemed the track to be clear of other users, a movement authority is given to the train through the Eurobalises. Due to the point based design of level 1, optical trackside signals are in use unless a system provides semi-continuous infill. The infill makes possible temporary continuous communication and can be achieved for example with Euroloop or by radio. Use of infill improves the safety and ease of operation due to the train receiving updates as soon as the trackside has cleared the track.[5]

The trains on-board systems calculate the speed profile for the track section the movement authority covers. The information about the track is received with the

movement authority and that information is used with the known characteristics of the train to calculate the maximum speed at any given point. The ETCS on-board will also compare the speed profile with the current speed to monitor and make sure the train does not exceed the speed limit.[5]

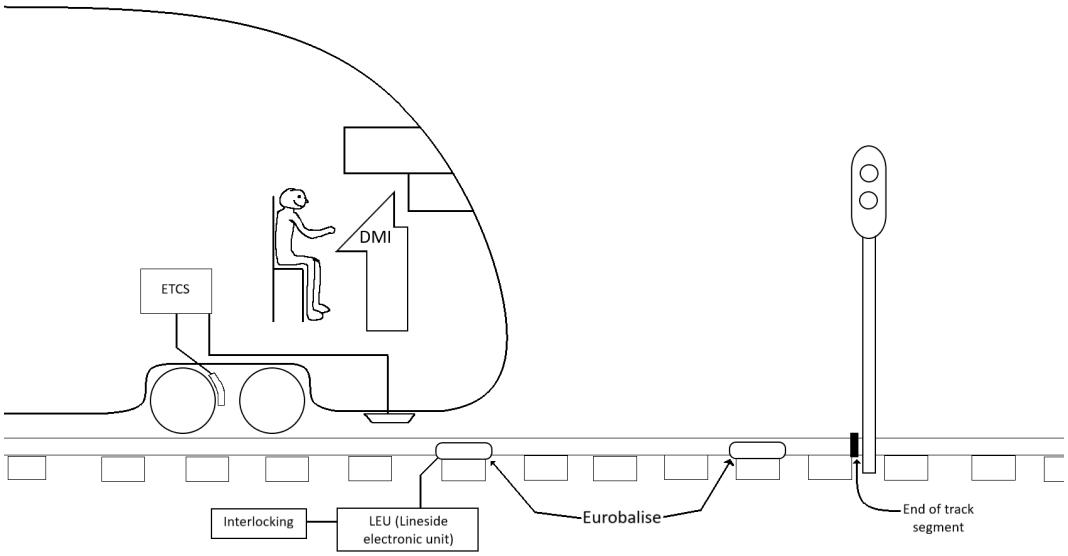

Figure 3: ERTMS/ETCS level 1

Level 2: The big difference between level 2 and level 1 is moving to radio based continuous transmission. Most of the other systems work just like in level 1, where trackside equipment is relied on for movement authorities, interlocking and train integrity. One new system needs to be added to the trackside called radio block centre (RBC) which is in charge of the radio communications between the train and trackside equipment. On the train an on-board unit (OBU) is the entity that handles the communication with the RBC.[5]

Even though a continuous radio communication is available between the train and trackside, Eurobalises are still in use. However their duty has changed from providing trackside data to providing location information to the train.[5] This allows the train to calibrate its location accurately at every balise it reads. Location data is important on level 2 because the RBC needs to be able to track the train[16]. Trackside optical signals are optional on level 2, therefore the driver is reliant on the on-board systems to present accurate information specially regarding movement authority left for the train. Aside from Eurobalises the location of the train is left to the underlying systems, which are not in the scope of ERTMS.[5]

Level 3: Level 3 is also radio based like level 2, however on level 3 two critical systems will switch from trackside systems to the scope of ERTMS[4]. The first

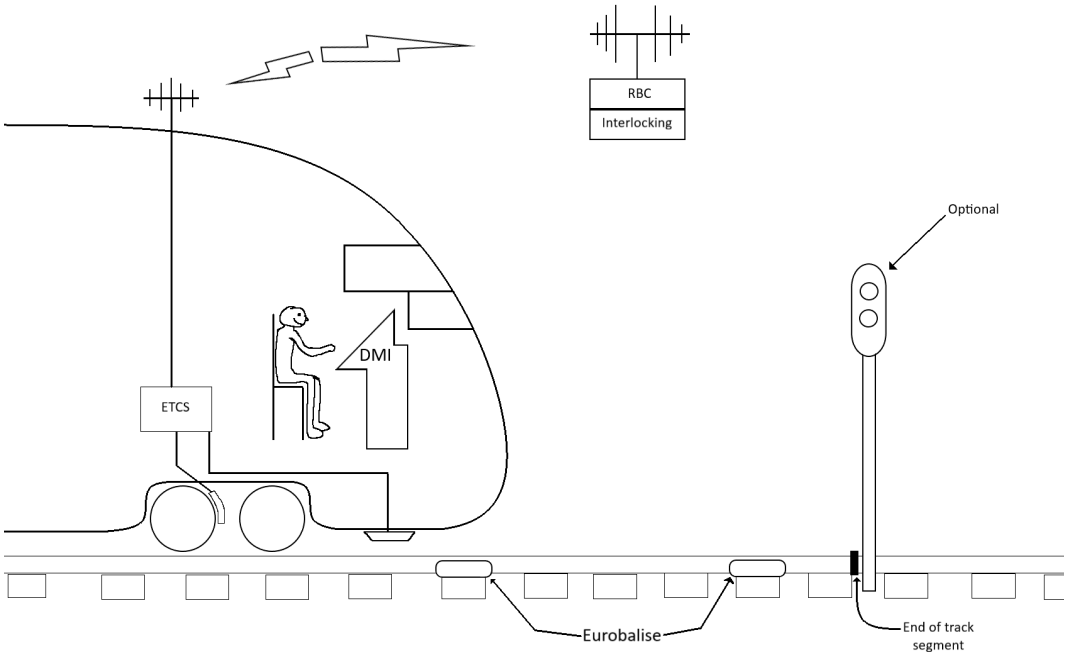

Figure 4: ERTMS/ETCS level 2

one is tracking of the train. Instead of an trackside system, e.g. axle counters, the RBC is responsible for the location of the train. This should be done in co-operation with train, therefore balises can still be used in assisting the tracking of the train. However other systems are most likely needed to provide continuous highly accurate tracking.

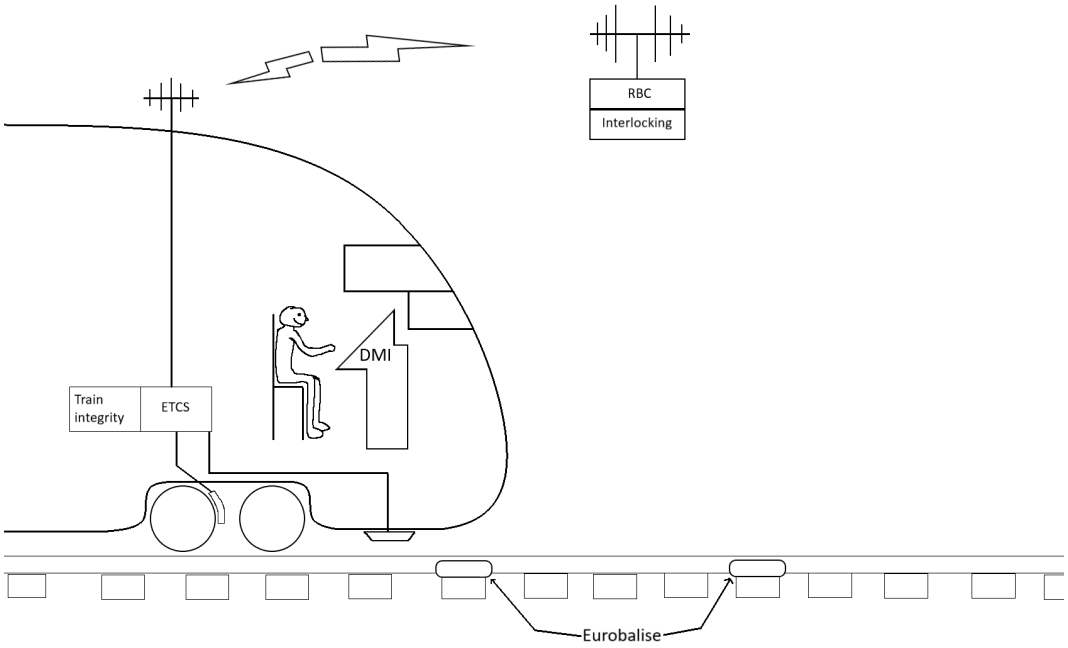

Figure 5: ERTMS/ETCS level 3

The second system is train integrity. Integrity checking will move from trackside systems to on-board systems. This means the train itself is in charge of checking and communicating its integrity to the RBC.[5] Due to integrity and tracking no longer being trackside dependent, it is possible to decommission some equipment used in interlocking, e.g. axle counters and track circuits. Currently these are used to make sure the train has completely left the track section.[17]

Hybrid level 3: ERTMS/ETCS hybrid level 3 is a version where there is support for both level 3 trains and level 2 trains without on-board integrity checking. This is achieved by keeping a limited number of trackside integrity systems in place that the level 2 trains can use. Mean while trains equipped with level 3 capabilities will be able run on fixed virtual blocks allowing for the splitting of the track section to smaller lengths without increasing the trackside equipment.[6]

There are several operational modes for ETCS that will be used in different situations. The modes differ in what capabilities the train can use and how the control is divided between the driver and the ETCS system. The modes in use are:

- Full Supervision (FS)

- Limited Supervision (LS)
- On Sight (OS)
- Staff Responsible (SR)
- Shunting (SH)
- Unfitted (UN)
- Passive Shunting (PS)
- Sleeping (SL)
- Stand By (SB)
- Trip (TR)
- Post Trip (PT)
- System Failure (SF)
- Isolation (IS)
- No Power (NP)
- Non Leading (NL)
- National System (SN)
- Reversing (RV)

Full Supervision (FS) is the normal operating mode for ETCS. FS mode activates by default when all the necessary train and track information has been received. In this mode all of the ETCS capabilities are in use.[5, 17]

Limited supervision (LS) is used in track sections that have some signals that are not overseen by the ETCS system. This mode is mostly for track sections that do not have a national system and are being upgraded to meet ERTMS/ETCS standards. The driver is in charge of the operations of the train due to lack of supervision of all systems by ETCS.[5, 17]

On Sight (OS) mode is in use when a train needs to move to a track section where availability cannot be confirmed. The ETCS system will be overseeing most systems, however track availability detection is left to the driver. Therefore the driver needs to use increased care in driving and be able to stop the train within the visible section of the track.[5, 17]

Staff Responsible (SR) as the name suggests allows the train to be moved in an ERTMS/ETCS zone under the drivers responsibility. SR mode can be used during the awakening of the train, to override stop signals or during a trackside system failure. The distance a train can move in SR mode can be set with different items. It can for example be given a list of balises that can be ran over or there can be a national value for the maximum distance. Even though the driver is responsible during this distance, the ETCS system will still be supervising speed limits and can trigger braking if needed.[5, 17]

Shunting (SH) is used for changing the train configuration, e.g. removing or adding railroad cars. In SH mode no train information is required and movement is limited with balise lists or special balise messages. Shunting also often has a lower speed limit (35 km/h in Finland) and the limit is set by the national operator of the railways. [5, 17]

Unfitted (UN) mode is used when there is no ETCS or national system available. This can be due to the track section completely lacking the systems or the system

being unavailable at that time. Because there is no control system available, the driver is responsible for the movement of the train and the speed limit is set to a national standard value (80 km/h in Finland).[5, 17]

Passive Shunting (PS) mode will be used when the engine is used as a slave engine in a dual engine setup without remote control. This applies also to trains with two cabins during a cabin change. In passive shunting the lead engine needs to be in shunting mode. While in PS mode the ETCS system will not do any train control actions and will ignore any errors that arise. Possible errors will be handled when leaving the PS mode. [5, 17]

Sleeping (SL) mode is for a remote controlled slave engine. The slave engine has no responsibility in train control actions as it is being remote controlled and there is no driver present in the engine. In SL mode the ETCS system can still contact the RBC if requested, or in case of a safety critical error in the ETCS/ERTMS equipment.[5, 17]

Stand By (SB) is the default mode where the ERTMS/ETCS equipment on board the train will be awoken. The system will gather necessary train and driver information to begin operation. During the SB mode the ETCS system is responsible for keeping the train still.[5, 17]

Trip (TR) mode is applied when the train moves past its current movement authority. In trip mode the ETCS system applies the emergency brakes to bring the train to a standstill and will keep the train in a standstill. In order to change the operating mode from TR and release the brakes the driver needs to acknowledge the trip.[5, 17]

Post Trip (PT) will be entered after a trip has been acknowledged. The train will be able move backwards the distance given as a national value (200 m in Finland). While in PT mode the train will only be able to move backwards and balise errors will be ignored. The driver will be responsible for the backwards movement, however the ETCS will supervise that the distance moved will not exceed the national value.[5, 17]

System Failure (SF) mode will be activated when the ETCS discovers a fault that affects safety. The command to apply the emergency brakes will be given by the ETCS and the responsibility of ETCS will be only to keep the emergency brakes on.[5, 17]

When a train is in isolation (IS) mode the ETCS system will be disengaged from the brakes of the train. This isolation needs to be done physically. In IS mode other system can also be disengaged from the ETCS equipment. While in IS mode the ETCS system has no responsibilities and moving to the mode is under the drivers full responsibility. Isolation can be used for example during maintenance.[5, 17]

In No Power (NP) mode the ETCS equipment is not powered. The ETCS will be commanding emergency brakes to be on permanently. It is possible to for the ETCS system to monitor cold movement (engine acts as a wagon) with systems connected to an auxiliary power supply. In case cold movement is necessary, the brake command will have to be overridden externally.[5, 17]

Non Leading (NL) mode is for managing a slave engine not remote controlled by the leading engine. In this case the slave engine has its own driver. As in SL mode, the slave engines ETCS systems will not perform movement supervision, however on

levels 2 and 3 the engine needs to inform its position to the RBC. Due to the lack of ETCS supervision, the driver of the slave engine will be responsible for following the orders displayed on the DMI. NL mode can be used for example when assisting a train stuck going uphill.[5, 17]

National System (SN) mode enables the use of ETCS resources while using a NTC system through STM. The responsibility of the train control will be on the national system and ETCS will only monitor possible level changes.[5, 17]

Reversing (RV) is reserved for only specified sections of the track, such as in long tunnels. RV mode is used to escape a dangerous situation as fast as possible. The on-board systems will monitor the speed and distance reversed, but the driver is in charge of the trains movement. In RV mode balise reading errors will be ignored.[5, 17]

ERTMS will offer several benefits including increased interoperability, capacity and safety. Interoperability through a unified system makes it possible to take one single train across Europe without facing signalling issues. Currently the national systems in Europe can hinder the competitiveness of railways, therefore having an unified system would allow trains to compete with other transportation [18]. This combined with the current maximum supported speed of 500 km/h [19], if achieved, will make railways be able to be more competitive with airlines within Europe.

Increased safety will come from having ERTMS perform automatic train protection (ATP)[18]. This constant monitoring lets the driver react to errors or mistakes faster and as the system has access to the brakes it can also perform an emergency stop if necessary. In addition on ETCS levels 2 and 3 there is no need to rely on visual trackside signals, therefore the safety is increased as the movement authority information is available regardless of weather.

With ETCS level 3 operation it is possible to change the interlocking system. Now a train always occupies a certain section of the track, meaning no other train can enter that section. With ETCS level 3 and the upgraded tracking and integrity systems on board the train it is possible to use moving block interlocking. This means the safety zone around a train is not tied to a section of a track, but the moving train. The zone will take to account the train information and speed of the train to create an area around the train where no other train can enter without tripping the system. With moving block operation it is possible to decrease the distance between trains therefore increasing the capacity of the line.

In figure 6 the high level depiction of systems is shown as presented in subset-26[5]. In this figure the red rectangle presents the main focus of what this thesis will look at.

2.1.2 Status in Finland

The current train control system in use in Finland is called "Junakulunvalvonta" (JKV), and is internationally known as ATP-VR/RHK[20]. This system was first brought to commercial use in 1995 on the track between Kupittaa and Kirkkonummi. The implementation schedule of JKV was sped up on the rest of the track sections in Finland due to accidents happening in 1996 and 1998. By year 2009 most of the

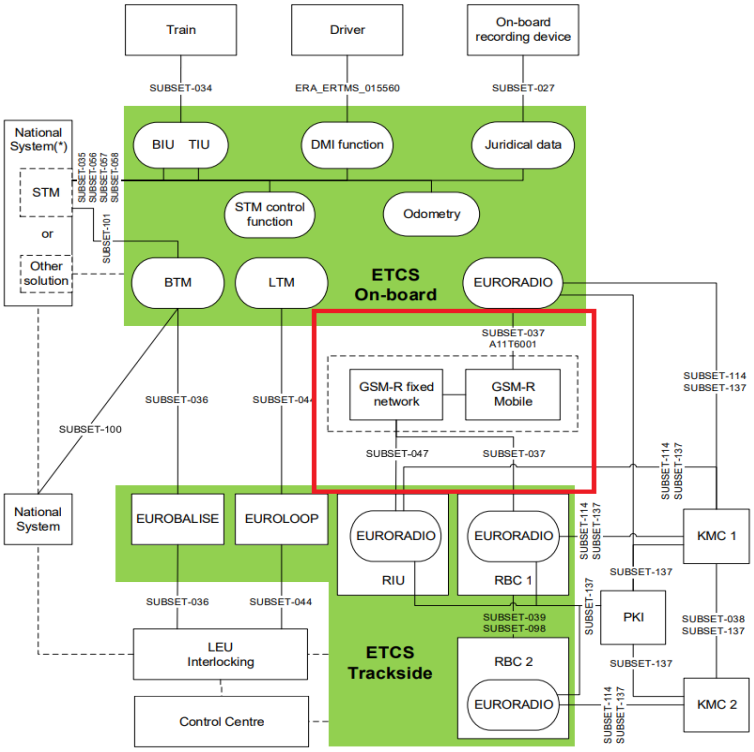

Figure 6: ETCS system level figure

state owned track was using the JKV system and currently 98% of traffic is operated on JKV enabled track sections[21].

The JKV system is similar to ETCS level 1 and is based on non-continuous transfer of data through balises. Even though they are similar, JKV is better optimised to fit the needs of Finland compared to ETCS level 1 as the system was designed specifically for it[21]. The differences between JKV and ETCS level 1 consist of options such as individual speed profiles for trains based on the train number and the availability to increase speed before certain hills to avoid the train becoming stuck.[20] Due to these similarities Finland plans to skip ETCS level 1 and upgrade straight to at least level 2. This project to upgrade Finnish rail systems is called Digirail.[9]

A part of ERTMS is the GSM-R network which currently does not exist in Finland. GSM-R was replaced by VIRVE (viranomaisverkko, government official radio) between 2018-2019 as part of upgrading the radio network. This network is used as a speech radio between the train and traffic control and there are some mobile device applications used for train dispatching, however VIRVE has not been used for train control commands. Having no GSM-R network gives Finland a good position to go straight to Future Railway Mobile Communication System (FRMCS) as no migration scenarios with GSM-R have to be considered. Building FRMCS in Finland can also take an interesting path as there is heavy favor in Finland to using commercial networks as the base. This is very different from other European countries, where dedicated networks have been the go-to option. In Finland there is

already an extensive commercial network so being able to use it for FRMCS network would offer cost benefits of not having to upkeep and build a dedicated network. [21]

The Digirail project aims to upgrade all of the railways in Finland that are running JKV. The project started in May 2019 with a clarification phase followed by a preparation phase ending in May 2021. Digirail has advanced to development and verification phase that is planned to last until 2027 and during this phase the first commercial track will be implemented in Tampere - Pori/Rauma during 2025-2026. The target is to reach at least ETCS level 2 and the option for ETCS hybrid level 3 is still open.[21, 9]

2.2 Railway wireless systems

This section introduces the wireless systems that are in use in railway operations and what has been planned for the future. The key technologies that are talked about are GSM-R which will be in subsection 2.2.1 and Future Railway Mobile Communications System will be in subsection 2.2.2.

2.2.1 GSM-R

Railways have always had strict quality-of-service (QoS) requirements. High QoS is needed for critical services and high speed scenarios where missing messages can lead to unnecessary applying of brakes or accidents at worst. This combined with wanting to use cost effective equipment lead to the development of Global System for Mobile Communication for railways (GSM-R). GSM-R, as the name suggests, is based on GSM but it has some added features that are described in Table 1.[22] Even though GSM-R was developed for the use of ETCS, it gained popularity and achieved high acceptance outside of Europe fast for being the most reliable network of its time. In 2020 there was almost 150 000 km of train lines with GSM-R in Europe and 250 000 km outside of Europe. Most of the track lines using GSM-R outside of Europe is located in China, due to use of Chinese Train Control System (CTCS) which is based on ETCS. [7]

Table 1: Table of added functionalities in GSM-R [22].

Voice group call service	Makes creating group calls between for example trains and base stations, or train staff and trackside staff possible.
Voice broadcast service	Allows the broadcasting of voice messages to certain groups. Used for prerecorded messages and announcements.
Enhanced multilevel precedence and preemption	Defines the priority of the users and is used to make sure emergency calls have high performance.
Functional addressing	Functions are given addresses which can be used to address the train, instead of having a permanent identifier.
Location dependent addressing	Function calls from the train can be addressed based on location of the train.
Shunting mode	Used for communication in shunting operations.

GSM-R uses frequency bands around 900 MHz. In Europe the bandwidth is divided so that uplink is on 876 - 880 MHz and downlink is on 921 - 925 MHz. The bandwidth is divided into 21 channels of 200 kHz however two channels are often not in use to achieve separation and protection from interference, leaving 19 channels for use. Each of these channels have a maximum transmission speed of 9.6 kbit/s.[11] GSM-R achieves message latency in the order of 400 ms and connection creation of 7 seconds [23].

The statistics show that GSM-R has been a successful system. However the capabilities that were enough before will not be enough in the future. Communications technology has advanced in leaps in the past 20 years and many aspects of GSM-R have become limiting factors.[7] Due to being in the very contested band of 900 MHz GSM-R can face interference issues. Public operators want to also have good coverage around tracks for their customers which increases the chance of interference if it is not properly planned. A study by Sun et al. [24] investigated power levels needed to maintain the QoS standards set for ETCS when there is a competing network. Sun et al. suggested that Δ P should be over 16 dB to ensure QoS and noted that when Δ P dropped to 7 dB some of the QoS requirements were no longer met.

Capacity and capability will also limit the use of more modern technologies. Having available only 19 channels with 200 kHz bandwidth is very limiting to the capacity of the network. According to an interview that was had with a German ERTMS specialist this has already come to existence in a railway station where not all trains were able to connect to the RBC. Being a system designed for voice communication GSM capabilities are not designed for data traffic and is mostly suited for low demand applications [22]. Having a maximum link of 9.6 kbit/s restricts the use of images and video and real-time applications struggle with 400 ms latency. Moreover the 7 second connection creation time hinders the speed of emergency services.[11] Capacity issues could be helped with more bandwidth, however the availability of bandwidth in the 900 MHz range is very limited. In Finland for example all of the neighbouring channels are reserved[25] offering no ease on bandwidth limitations.

In addition to the aforementioned limitations GSM-R offers no passenger services. This might not have been an issue when the system was designed, however with modern trends using mobile devices has become common place. The lack of passenger service support lowers the user experience of passengers. In [11] it was calculated that a passenger train with maximum capacity of 1114 passengers would require at least 168.44 Mbit/s, which is orders of magnitude higher than what is currently available.

Communications technology has advanced from 2G to 5G during the existence of GSM-R. This progress is however making GSM-R obsolete as an older system. The end of support from suppliers for GSM-R is expected around 2030[7]. In preparation for this the development of the next railway communication system began in 2014 by Union of Railways (UIC) under the name of Future Railway Mobile Communication System (FRMCS).[22]

2.2.2 Future Railway Mobile Communications System

The new Future Railway Mobile Communications System (FRMCS) is still under development, however the UIC has released migration scenarios [26] and user requirements [28]. The user requirements specification (URS) leaves it open about what technologies should be used and only states that FRMCS should support applications independently of the network. This means for now there is no requirement about what technology the new system will use as its base. It has been an active research topic how FRMCS could be done using 4G or 5G. [11, 29, 30, 31, 32, 33]

Either of 4G or 5G will be a huge improvement over GSM. Taking speeds from 9.6 kbit/s to at least dozens, maybe hundreds of Mbit/s. Latency will also be reduced from 400ms to under 100ms. Call setting time is also defined in [36] to be at most 2.5s for group calls, which significantly lower than 7s of GSM-R. While 5G solutions are waiting for the technology to mature and be more widely available, some 4G solutions have already been built. In South Korea the first LTE-R network was implemented at the end of 2017[34].

The biggest differences for railways between 4G and 5G are support for IoT and sheer throughput. According to Chen et al. in [11] even LTE-A might not be enough to support Railway Internet of Things (RIoT) or real-time video surveillance. Real-time video is required in a few cases in the user requirements for FRMCS[28]. So it seems that current projects moving forward from GSM-R will use the currently available LTE technology, While projects in a few years will most likely use 5G.

Whether it be 4G or 5G, there has been discussions if railways should have their own dedicated network. In many countries using ERTMS the GSM-R part has been a dedicated network only for railways. However a dedicated network is costly to implement and upkeep, so in Finland the possibility of using commercial mobile network operators (MNO) has been looked at as a possibility[21]. As part of the Digirail project a study has been done regarding the current state of coverage and QoS of MNOs for trains. While the study was not yet released as public during the writing of this thesis, there was a press release given about it. The press release [35] stated that the current commercial networks (4G) easily fulfill the current requirements for the train control needs.

As mentioned before, the FRMCS specification might not be published yet, however 3rd Generation Partnership Project (3GPP) has worked with UIC and ERA to have FRMCS built into 3GPP releases. Currently 3GPP release 17 has TR 22.889 [36] which defines use cases for FRMCS operation and basic information about FRMCS. The features listed in TR 22.889 for FRMCS are:

- Emergency group communication, train control data and video service
- High speed moving railway environment connectivity
- Low latency and high reliable data and video service
- Train management and monitoring in real time
- Location tracking
- Interworking to GSM-R system

This list of course has similarities with what was wanted from GSM-R. However

additions have been made to include high speed trains, video service and low latency capabilities.

The basic structure of FRMCS system is show in figure 7. In this figure you can see the main parts of the system, which are on-board applications, FRMCS on-board system, core network services, trackside FRMCS service and trackside applications. The on-board applications are connected to the FRMCS on-board system through the reference point OB_{APP}. This reference point consists of two points OB_{AUTH}, and FRMCS service session interface (FSSI)[37]. Through OB_{AUTH} the railway applications will authenticate to the FRMCS Mobile Gateway, and allows the mobile gateway to inform the applications of e.g. the server used for service sessions. FSSI will be responsible for achieving functions such as registration to the Mission Critical services (MCX), configuration management, security, MCPTT functions, MCData functions, and MCVideo functions.[37]

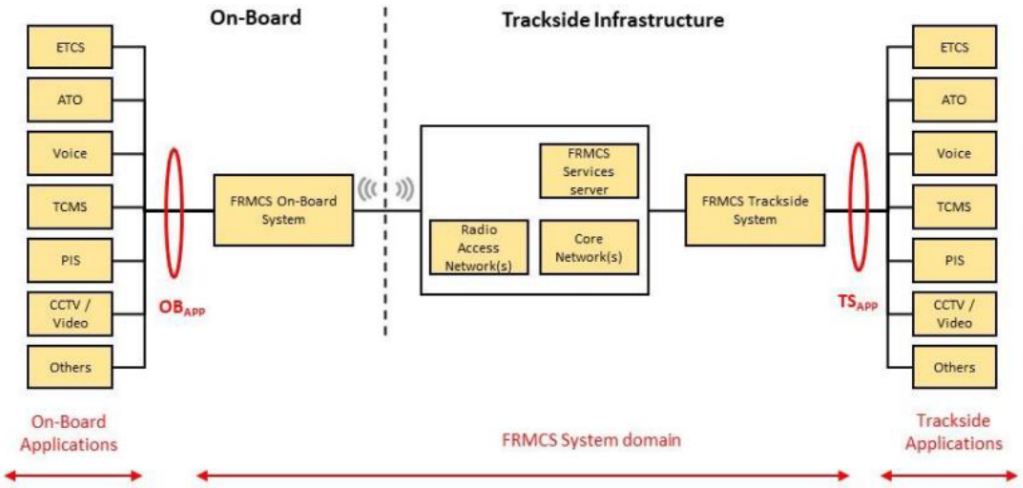

Figure 7: FRMCS system domain

One of the main new things that FRMCS will bring with it is the Mission Critical Service (MCX) which serves as the base for Mission Critical Push-to-talk (MCPTT), Mission Critical Data (MCData) and Mission Critical Video (MCVideo). These services would be running on a MCX server that is located in the network and MCX clients would be present in all systems that need to use FRMCS. In figures 8 and 9 one possibility of how this might be done has been presented. It should however be noted that FRMCS version 1 has not been released yet, and these pictures are the assumptions of the system by Finnish Transport Infrastructure Agency (FTIA) at the time of writing this thesis.

Figures 8 and 9 show that there is a difference between the MCPTT and MCData user plane and control plane. In this scenario the voice application has tight coupling, meaning the sender knows who they are talking with. This comes directly from the voice application being MCPTT therefore it is already part of the MCX system. The data application however would be loose coupling, so the application would not know

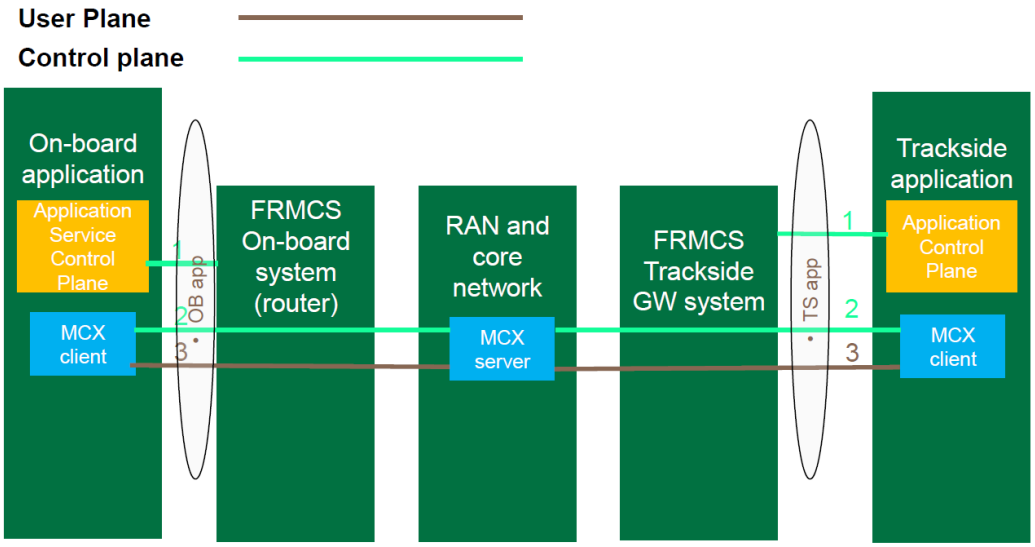

Figure 8: Voice application user/control plane

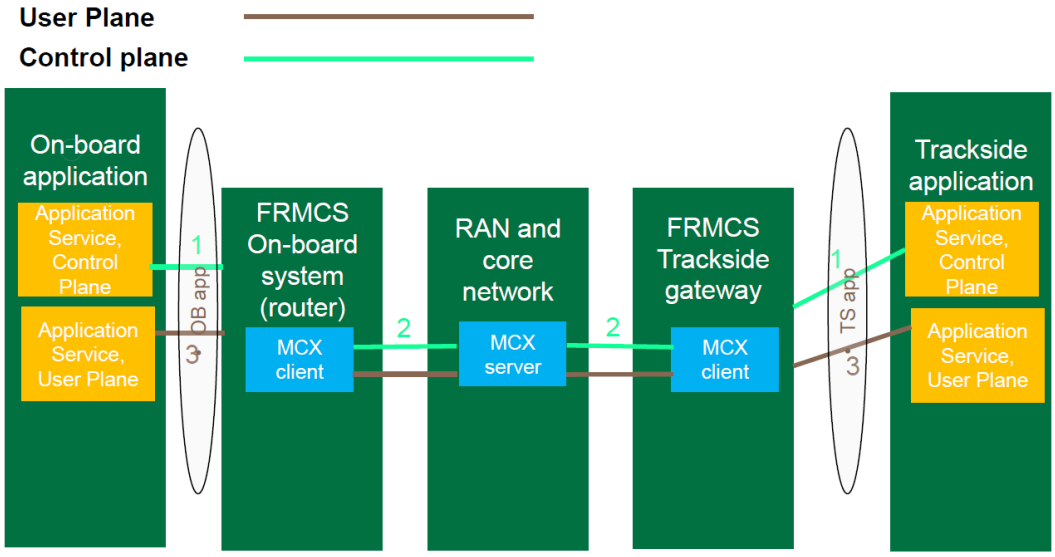

Figure 9: Data application user/control plane

where the data is sent. The data application being loose coupling is argued for in the ETSI TR 103 459 V1.2.1 [37] by saying this will support the development of applications independently of the transmission system.

MCX requires applications that communicate with it to be authenticated. This means that all applications will need to register with the MCX client and during this step their public identity is bound to the MC service identity. This process is called local binding.[38] However this would be an issue with applications not aware or not capable of mission critical communications. Therefore MCData has built in an IP connectivity option which allows data hosts to use the MCData as a gateway over the MCX system. How this works is described in more detail in ETSI TS 123.282 [39].

MCX also has common security requirements defined for all of the services. The full list of requirements can be found in 3GPP TS 22.280[38]. Here will be presented a list of some of the common requirements.

1 The MCX Service shall provide a means to support the confidentiality and integrity of all user traffic and signalling at the application layer.
2 The MCX Service shall support MCX User with globally unique identities, independent of the mobile subscriber identity (IMSI) assigned by a 3GPP network operator to UEs.
3 The MCX Service shall require authentication of the MCX User before service access to all authorized MCX Service features is granted.
4 The MCX Service shall provide a means to support end-to-end security for all media traffic transmitted between MCX UEs.
5 End-to-end security shall be supported both within and without network coverage and regardless of whether the traffic is transmitted directly or via the network infrastructure.
6 The MCX Service shall provide a means by which an MCX UE can require authentication of the MCX Service.
7 An MCX User who has a profile that has been deleted or suspended shall be prevented from using that MCX Service User Profile to access the MCX Service.
8 MCX UEs operating off the network shall be capable of authenticating the sender of messages carrying Location and identity information.

This list of requirements is presented here so we can compare the requirements later to those presented in other standards.

2.3 Chapter 2 summary

Chapter 2 of the thesis has investigated the modern railway systems operational in Europe, with special focus on systems in use in Finland. The systems we cover are the European Railway Traffic Management System (ERTMS), the European Train Control System (ETCS) and “Junakulunvalvonta” (JKV). Chapter 2 provides the base knowledge for understanding the operational modes and technical terms related to modern railway systems.

The most important aspects for ERTMS are safety and interoperability. Before, and even now to some extent, all countries could have their own train control systems, which makes it more complex for trains to travel over borders. ERTMS has been designed to standardize the railway operations to allow easy travelling across Europe. ERTMS is often depicted with levels. The levels give an idea of what technologies have been used with the safety system.

Change in railways is slow. It can easily take decades to change systems as they have been designed with long lifecycles in mind. This means that also parts of ERTMS could also be considered old technology. One example of this is the GSM-R communication system. Compared to the commercial networks that have started to decommission 3G networks, the railways are still stuck in 2G. The newest (autumn 2023) specification for ERTMS still has 2G as the main network option. However the 2023 specification opens the door to FRMCS albeit only for the dedicated version. While it is not yet in the specification, Finland is trying to be the forerunner of allowing the use of commercial non railway dedicated networks for ERTMS. As there is no GSM-R network in Finland, the commercial networks would be an option to lower the cost of implementing ERTMS due to not having to build a costly and most likely temporary solution as the FRMCS specification is changing.

The higher levels of operation in ERTMS are reliant on wireless communication. GSM-R has encountered limitations concerning bandwidth, capacity, and modern data demands of passenger services. Therefore it is important to be able to make the change to a more modern solution. The development of FRMCS, still ongoing, presents two potential technology options: 4G and 5G. While some regions have already implemented 4G solutions, 5G technology is expected to provide greater throughput and support for advanced services.

While the actual safety functionality has no need for a lot of bandwidth, the extra bandwidth can used for auxiliary services. FRMCS will also update some security capabilities of the network. Some of these upgrades will come from updated processes and some are related to using a newer technology for the networks.

3 Railway safety and security

This section will be talking about the safety and security standards related to railways. In safety standards we take a look at the EN 5012X series and EN 50159. For security the main standard that will be looked at is the newly released CENELEC TS 50701 railway cybersecurity technical specification.

3.1 Safety

Railway safety is a highly regulated process with several standards and guidelines on how work should be done. For example FTIA has an 18 pages long list of documents that should be followed[40]. There are several CENELEC standards also such as EN 50126 series focused on the total railway system, EN 50128 focusing on signalling software, and EN 50129 focusing on signalling system safety. The basic function of safety is to protect humans from machines.

Reliability, Availability, Maintainability and Security (RAMS) process for railways is defined in EN 50126-1[41]. The idea of RAMS is to use engineering concepts and tools throughout the life cycle of a system to ensure a certain level of availability and safety over a period of time. The RAMS process often uses risk based approach to achieve this by identifying risks, then deriving requirements and implementing measures of mitigation. According to EN 50126-1[41] risk is a combination of two elements, the expected frequency and the severity of loss. Loss can be anything from human injuries, property damage or environmental damage.

In risk reduction there are in general two ways to achieve it, reducing the severity of loss or decreasing the frequency. Specifically related to safety there is a three step process to get the risk to an acceptable level. The steps in order are: avoiding the hazard completely, ensure low frequency and minimise consequences. A railway concept is safe failure, where failures lead the operation towards a more safe option. Often this for trains means stopping the train, as a stopped train is safer than a moving one. However even for this there is an exception for a burning train, as stopping a burning train inside a tunnel for example would not result in a more safe situation. Therefore the safe status of the system needs to be considered under all circumstances. [41]

In the case of RAM risks the two principal ways of reduction are improving reliability and improving availability. Reliability increase results in reduction of frequency while availability increase makes the loss smaller when it occurs. Measures that can be taken to improve reliability can be such as preventative maintenance, system tolerance level designing, using components in their optimal range, or good quality management practices. For increasing availability measures such as duplicate systems, degraded mode operation, sufficient resources, or higher maintainability can be used. These measures can of course be used in combination with each other.[41]

Another aspect that is brought up in EN 50126-1 is the life cycle V-model. The V-model depicts the interrelation of life cycle stages and tasks. The V-model is presented in figure 10. In total there are 12 steps in the model and it can be split into roughly three portions: development, assembly/installation, and operation. The

V-model is an important and recognised life cycle process in the railway sector.

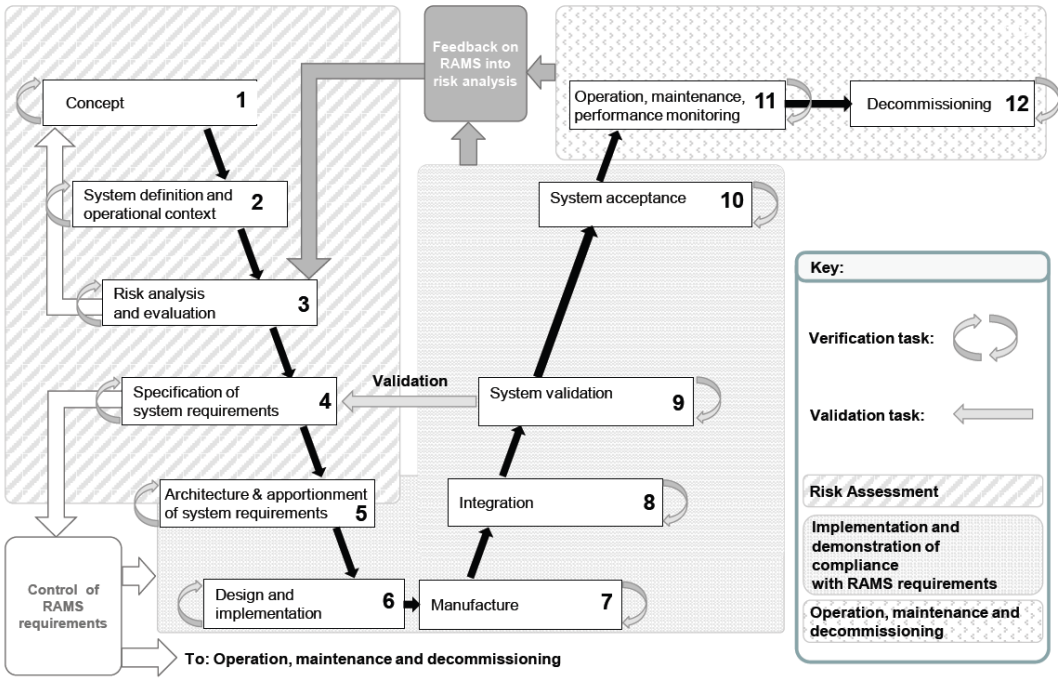

Figure 10: RAMS V-model as presented in EN 50126-1

In EN 50126-1 the tasks that need to be done in each life cycle step are defined in detail. Moreover the concept of Independent Safety Assessment is defined. The point of independent safety assessment is to evaluate and judge if the safety management process has been completed in sufficient adequacy. Independent safety assessment is based on three main deliverables: independent safety assessment plan, record of findings, and independent safety assessment report.[41]

The requirements for the entity carrying out the independent safety assessment is defined in EN 50126-2. One of the main requirements for an independent safety assessor (ISA) is of course being an outside and independent entity from project management. ISA also needs to, for example, have sufficient competence in the technologies being assessed and the EN 50126 standard. The full of responsibilities and competencies can be found in EN 50126-2 annex G.[42]

Other key items defined in EN 50126-2 are deriving safety integrity levels (SIL) and safety requirements specification. SIL is represented with a value from 0 to 4 and it is based on the tolerable functional failure rate of the function in question. As such a higher SIL can be thought of as higher confidence that the system is not corrupted by random or systematic failures. However SIL is only to be used in functional safety of electronic architectures, and different methods, such as codes of practice, should be used for non-electronic systems.[42]

Safety requirements are split into three categories. First functional safety requirements cover the expected behaviour of safety related functions and the behaviour in failure cases of those functions. Secondly the technical safety requirements consider the technical design and implementation of the system where potential hazards

are e.g. fire, voltage or structural integrity. These requirements often rise from regulations and standards. Last the operational and maintenance safety are covered by contextual safety requirements.[42]

The third part of EN 50126 standard is the EN 50126-3 and it is an application guide of RAMS in rolling stock. EN 50126-3 expands some of the aspects from 50126-1 and makes them clearer for the case of rolling stock. Consideration is also shown for life cycle cost which can be linked to RAM as often one of the highest cost during a product life cycle is maintenance.[43] As such this part of the standard is the least relevant to the subject of this thesis.

The EN 50128 standard defines the procedure for railway safety related software. This includes the development, deployment and maintenance of software, and software safety integrity levels (SSIL). SSIL is defined the same as SIL in numbers from 0 to 4. Measures required for each SSIL are defined as part of the standard.[44]

SSIL is based on what has been done before and during the software development process. This is a clear difference from SIL and stems from the problem of defining functional failure rate for a computer program. Therefore instead of representing a failure rate, SSIL represents the level of software development practices used.[44]

EN 50128 also has its own V-model similar to what was introduced in 50126-1. The basic structure is the same, starting from requirements, then architecture, design, implementation, testing, integration, validation and lastly maintenance.[44] The tasks during these phases might differ in naming, but can be considered as the software equivalent of the tasks in 50126-1.

There is a total of 71 techniques presented for software development in EN 50128. Some of these are designed to tackle the same problems, such as different modelling options. One of the techniques that is considered mandatory on all SSIL over 0, is called defensive programming. This method includes sanity, range, and type checks for variables and configuration checking for itself. The aim of defensive programming is to ensure that the program can detect anomalies and handle them in a predetermined way.[44]

The standard EN 50129 is focused on the system safety of railway signalling systems. It covers the requirements for the quality and safety management, and the organisation structure that was also presented in EN 50126-2. Even though many of the subjects covered in EN 50129 have been introduced before as parts of other standards, this standard brings forth some new subjects also. For example safety-related application conditions (SRACs) are introduced. In addition to SRACs there is a detailed description of the Safety Case that is required for system safety evaluation.[45]

Safety-related application conditions are used when the system under consideration and the whole system are integrated. The established conditions and assumptions that are required to mitigate risks in this scenario are called SRACs. SRACs should be always tied to a hazard that they are used to mitigate. The need for SRACs rise from hazards that can not be handled adequately within one part of the complete system.[45]

The complete system will be evaluated in a Safety Case. Safety case contains the evidence of quality and safety management, and evidence functional and technical

safety. The idea behind the safety case is to show and prove that the system as a whole fulfills the required standards and that it is safe to move to operation. It is possible to have safety cases for subsystems and they can be used as part of the safety case for the whole system.[45]

3.2 Security

As seen above the safety aspects of railways have been well standardised. However when looking from the security side things are very different. There are mentions of IT-security in 50129 and it is required that security measures are addressed in the safety case. However 50129 is fairly lax on that aspect and the key point is security risks are only managed if they affect safety, are foreseeable and cannot be easily excluded [45]. The other standard that covers some security aspects is EN 50159 that is focused on safety-related data communication. To bring security to railways there is a recent new addition to the security side, but it is not yet an actual standard. This document is the CENELEC technical specification 50701 (CLC/TS 50701). Outside of these documents there of course exists the operational technology (OT) standard series IEC 62443 and IT standards in 27000-series. CLC/TS 50701 however is one of the first railway specific cybersecurity technical specifications.

The EN 50159 standard [46] is focused on the transmission of safety related messages over a digital communication system. It introduces three categories of transmission systems to simplify the demonstration of safety. It can be said the EN 50159 covers the communication aspect of the safety case for the system. As such the requirements specified in EN 50159 however only cover a small portion of possible security threats and is not designed to be a comprehensive cybersecurity standard. It should be noted while in EN 50159 terms we are talking about unknown users or applications, it does not mean unauthorised or unknown to the owner of the communication system, merely unknown to the current user. For example in commercial mobile networks you do not know all the others using the same network.

The definition of different transmission categories has already been seen in this thesis in the FRMCS transmission schemes. These categories are given in EN 50159, with category 1 being for closed communication systems and categories 2 and 3 are for open communication systems. The category 1 systems generally have fixed and known number of equipment, the physical transmission system is fixed during the life cycle, and risk of unauthorised access is negligible. Categories 2 and 3 are open meaning all of the equipment connected might not be known to the user, there might be network control functions unknown to the user, and there might be unknown program elements that transform the data. The big difference between category 2 and 3 is that category 3 can be susceptible to unauthorised access.[46]

In the FRMCS transmission we defined a different approach for voice and data communication. Based on this short description of EN 50159 categories, we could argue that the voice communication would resemble category 1 and data communication category 2. The big difference being again that in data communication there might be an unknown application to the user doing something to the data the user sent. Whereas the voice communication had only known components. However this

might not hold as the FRMCS will most likely be assessed as a whole. Therefore specially in 5G there might by dynamic routing done by operators that the users aren't aware of, making it all at most category 2. In EN 50159 GSM-R for example is defined as a category 3 system[46].

The EN 50159 offers a range of defences to protect the safety-related messages. These defences are sequence numbers, time stamps, time-outs, identifiers for source and destination, feedback messages, identification procedure, safety codes, and cryptographic techniques.[46] While these defences are very relevant to the security of messages and are an important piece of the whole security, they can not cover the security of the entire system.

In an effort to bring railways to the modern cybersecurity era, the CLC/TS 50701 [47] was released in the summer of 2021. The aim of this CENELEC specification is to serve as a guideline in ensuring and demonstrating that the railway system has fulfilled the cybersecurity needs. While the CLC/TS 50701 contains new ideas, many aspects of it come from the IEC/EN IEC 62443 standard series.

There are several good concepts introduced in the CLC/TS 50701. These are such as Security Levels (SL), risk assessment for security risks, good design principles for security (section 2.4.1), and a link between security and EN 50126. This link to EN 50126 is the V-model, but in this case it is the cybersecurity version. This security V-model ties together the security actions that need to be taken to the life cycle stages of the RAMS life cycle. From the long list of activities we will take a closer look at these items: System under consideration (SuC) identification, zones and conduits, initial risk assessment, and detailed risk assessment.[47] Risk assessment has its own section (2.5) and the initial and detailed risk assessments will be talked about there.

The SuC identification is one the first activities that should be done in regards of security. It will be the basis for upcoming tasks such as the risk assessment[47]. On safety aspects the SuC identification is also used in this way[45, 41]. The SuC should be based on identifying the assets and functions in the system. After all of the assets and functions are identified we will have the SuC that can be partitioned to zones and conduits. A zone is a grouping of assets and a conduit represents a group of communication channels between zones. The idea behind zones and conduits is to group items that have similar security requirements.[47] While CLC/TS 50701 provides information on how the zoning and conduits should be done, a more detailed example based on the CLC/TS 50701 was presented by ENISA in early 2022[48]. In figure 11 a high level example zones and conduits model from CLC/TS 50701 is presented.

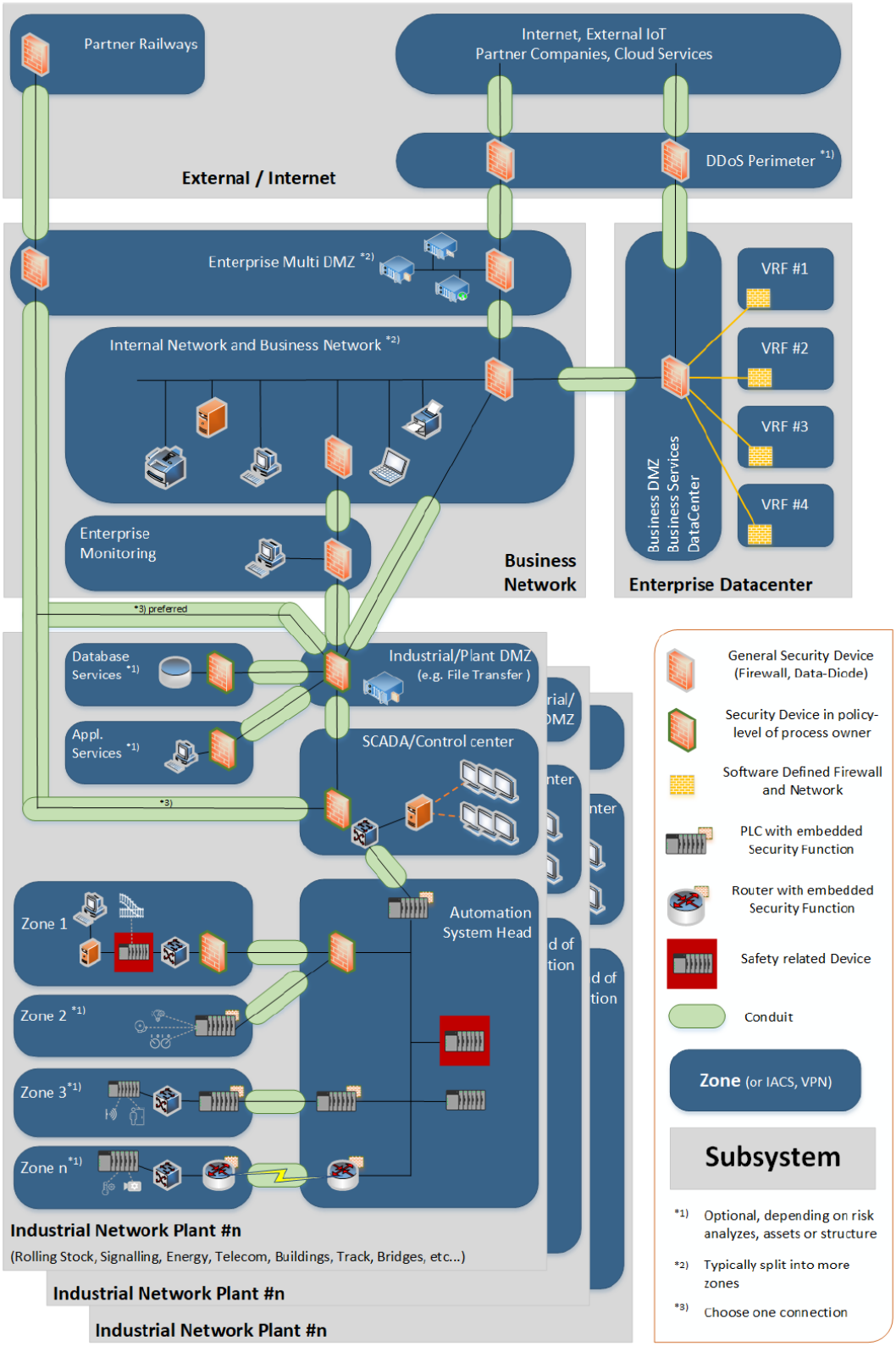

Figure 11: Example of a Zone and Conduit model as presented in CLC/TS 50701[47]

Every zone or asset will have a Security Level (SL) given to it. Security levels are the cybersecurity versions of safety integrity levels, meant to help in choosing the appropriate measures to protect the asset. The security levels shown in CLC/TS 50701 are based on the security levels from EN IEC 62443-3-2[47]. A visual presentation of what each security level means in terms of skills and resources is shown in figure 12. As with SIL, the security levels go from 0 to 4, with 0 meaning no protection needed. SL 1 is designed to protect against accidental or coincidental violations and incidents while SL 2-4 are for intentional violations with varying degree of skills and resources[49].

<table>
<tr><th>Security level</th><th>Incident type</th><th>Tools and methods</th><th>Resources</th><th>Skills</th><th>Motivation</th></tr>
<tr><td>SL 0</td><td colspan="5">No protection needed</td></tr>
<tr><td>SL 1</td><td>Accident or error</td><td></td><td></td><td></td><td></td></tr>
<tr><td>SL 2</td><td rowspan="3">Intentional</td><td>Public tools and methods</td><td>Low</td><td>Basic skills</td><td>Low</td></tr>
<tr><td>SL 3</td><td rowspan="2">Advanced tools and methods</td><td>Average</td><td rowspan="2">Advanced skills</td><td>Average</td></tr>
<tr><td>SL 4</td><td>Extensive</td><td>High</td></tr>
</table>

Figure 12: Security levels from EN IEC 62443-3-2 in a visual format.

In CLC/TS 50701 the security levels are created as vectors based on the seven requirement categories of EN IEC 62443-3-3. These categories are:

- Identification and authentication control (IAC)
- User control (UC)
- System integrity (SI)
- Data confidentiality (DC)
- Restricted data flow (RDF)
- Timely response to events (TRE)
- Resource availability (RA)

Security levels are can be either targets (SL-T), achieved (SL-A), or control system (SL-C). These identifiers are used to be able to compare if the current SL-A is enough to meet the set SL-T. The security level vector SL-T should be the deliverable of detailed risk assessment and could for example be SL = (3,3,3,1,3,3,1).[47] Moreover the EU funded Shift2Rail project has published their protection profiles for trackside and on board components. In the Shift2Rail documentation interlocking, RBC and many other critical assets were given a SL-T vector of (3,3,3,3,3,3,3)[50, 51]. This seems reasonable as some SL-4 requirements can be hard to implement in a safety system, such as *SR 3.3 RE (2) Security functionality verification during normal operation*[47].

While CLC/TS 50701 is a good step in the right direction it leaves room for improvement. For example key management is only shortly discussed as part of

other topics, and there is no cybersecurity management model for OT. A lot of the management side is left to be covered by standards such as ISO 27001. While leaving it up to other standards can be okay, it would have been a nice addition to have examples for OT (specifically railways) presented.

3.3 Cybersecurity

In this section the cybersecurity aspects and issues will be introduced. Latest cyber attacks towards railways will be looked at and possible issues arising in the future will be explored. Mitigation techniques in the form of design principles will also be introduced.

3.3.1 Cybersecurity status in railways

Cybersecurity awareness has been low in the railway sector. This was identified in studies such as [52, 10]. However both studies noted that the awareness is increasing. The ENISA study [10] reports that issues include problems such as reconciling between safety and security, on-going digital transformation, supply chain dependence, and geographically spread infrastructure. While these appear to be large problems there have not been many cyber attacks towards railways.

Lets look at the recent attacks or incidents in railways:

- Ukraine suffered an denial of service (DoS) attack from an advanced persistent threat (APT) actor. The attack targeted multiple critical infrastructure sectors in an attempt to destabilise the government in 2015.[53]
- Between 2015 and 2016 the UK railway network discovered several reconnaissance attacks to enable an APT attack.[54]
- Deutsche Bahn was attacked with the ransomware WannaCry in 2017. This attack affected the passenger information system.[55]
- Swedens Transport Agency and Transport Administration were attacked with DoS attacks in 2017. Two attacks on consecutive days were done targeting one of the targets. Systems that went down included railway related systems such as train location monitoring and ticket booking applications.[56]
- In 2018 a distributed DoS attack was done against the DSB ticketting systems preventing customers from purchasing tickets.[57]
- The data of users of the free Wi-Fi provided in UK railway stations was breached. Travel details of the users were published online, but the database did not seem to contain passwords.[58]
- A Swiss rail vehicle manufacturer Stadler was attacked with malware in 2020. Sensitive data may have been stolen from the breached systems.[59]
- In 2020 a ransomware attack was done against the Infrastructure Manager of Spain. Personal and business data was exposed.[60]
- The Dutch GSM-R network suffered an outage resulting from apparently a faulty patch in the GSM-R system. Train operation was disrupted for several hours.[61] While this was not an cyber attack, it was listed due to being closely relevant to the topic of this thesis.

While this list is not exhaustive, it holds the major incidents with public records. We can see that attacks have been mostly targeting the IT side of train operations and not the OT side. However there was a change in that during the writing of this thesis relating to Russia invading Ukraine. Attacks were done in Belarus to stop troops moving by train. The attacks targeted the train operation directly in order to

take the systems down and prevent automated train control[62, 63]. By the time this thesis is published these two attacks might be only a small sample of attacks, which is why the war and its effects are left open. It can be said though that these events have probably made the movement towards more security aware railways move at a faster pace.

3.3.2 Design principles

When we start to think about what can be done to prevent future attacks, we need to look at designing the systems. Cybersecurity design principles are core concepts that help you when designing the cybersecurity of a system. The CLC/TS 50701 presents a list of cybersecurity design principles. These principles are:

- Secure the weakest link
- Defence-in-depth
- Fail secure
- Grant least privilege
- Economize mechanism
- Authenticate requests
- Control access
- Assume secrets not safe
- Make security usable
- Promote privacy
- Audit and monitor
- Proportionality principle
- Precautionary principle
- Continuous protection
- Secure metadata
- Secure defaults
- Trusted components

While many items in this list of design principles are self explanatory, we will look a bit more closely on defence in depth, fail secure, authenticate requests and proportionality principle. Fail secure is the same concept as railways have had in fail safe, meaning a failure always leads to a more safe state. However for fail secure this can lead to contradicting commands as in a failure state a locked door should stay in the secure state locked, whereas safety might require it to be in the safer state of unlocked. According to CLC/TS 50701 in these cases safety should always overwrite the security needs[47].

The proportionality principle is used for balancing security and utility/usability. This becomes very important in railways where utility and usability are big factors for operation. This principle is based on identifying where security conflicts with usability. After being identified the possible loss from not implementing security measures will be compared to the loss in usability. While not directly related to usability or utility, cases of using more resources to mitigate a security risk than what the loss from that risk being realised is also included in this principle.[47] In short, all security actions taken should be proportional to the risk or loss in usability/utility.

The authenticate requests principle is one of the corner stones of cybersecurity. It means that where possible all users should be authenticated, whether they be human, software or device. There are several ways to authenticate users, such as passwords, signatures or certificates. It is also possible to have more than one authentication method in use at the same time, resulting in multifactor authentication. Authenticating requests is one of the core ideas in achieving defence in depth.[47]

Last principle we will be looking at is defence in depth. We will entertain us with a small analogy here, consider a thief looking to steal an expensive item from a mansion. The thief will be successful as long as they are faster than the police response time. So a top-of-the-line detection system alone will not be enough as even though the police might get a notification faster, it does not matter if the thief is gone by the time the police get there. Investing everything to slowing down the thief also will not stop the thief as while they will take longer to steal the item, as long as they are not detected they will have all the time in the world. So to protect your valuables you will need a combination of both to detect the thief and then slow them down enough that they can be caught.

This analogy shares the same idea that is behind defence in depth. That idea is that a single defensive measure or protection will not be able to able to stop an attack[47]. Therefore we should design our system so that no single violation or vulnerability will endanger the whole system, this same concept is present in the EN 50126 standards that no single point of failure should exist for safety[41]. The other core concept of defence in depth is to slow down the attacker with preventative measures and being able to detect the attacker to mitigate further issues[47]. In practice this means that every step the attacker takes should be protected with challenges to prevent a deeper intrusion or a lateral movement.

3.3.3 Cybersecurity challenges moving towards FRMCS

Railways are a cyberphysical system. Cyberphysical is used to describe networked systems that have the ability to sense and interact with the physical world[64]. In railways the physical side can be items like point machines, that are responsible for switching tracks, or rail crossings. These physical items are also spread on a very wide area which makes protecting those assets harder. Part of this is tackled by safety specification, as for example the state of a point machine is very critical to train operation, so often the system can detect offline/non-responsive assets and the state of the assets.

In section 2.1.2 we talked about how the current system in Finland is a non continuous transmission system. This close air-gap transmission system is considered category 1 transmission by the EN 50159[46]. In addition most trackside equipment is connected with wired networks (fibre, ethernet, copper) making the logical attack surface of the system fairly small. This means a big change when moving to a wireless system is the increase of attack surface to the system. While the trackside safety equipment will stay as wired connections, some of the mission critical data such as movement authority will move over to open radio transmission.

To protect this transmission over a category 3 network ERA has released the

EURORADIO[27] specification. It focuses on the integrity and authenticity of communication, as the contents of most ETCS messages are not confidential. For the integrity and authentication a Triple Data Encryption Algorithm (3DES) encrypted Message Authentication Code (MAC) is used. This encryption is based on a shared secret called KMAC that is used to as the base to create the MAC.[27] However there are things of concern presented in the EURORADIO subset.

High priority messages are sent without safety functionality as per section 5.6.1.4.[27]. This was also recognised in the study by Ruiter, Thomas and Chothia [65] where they tested the security functionalities of ERTMS protocols. They found out that while for normal messages it was not possible to insert or modify messages, or pretend to be an RBC or a train, it was possible to delete messages and insert high priority messages. The insertion of messages required an active connection between a train and RBC but if that connection was up the non secured high priority message would go through. Ruiter et al. suggest that to combat these two issues MAC should be used for high priority messages and that some counter be added to the messages to recognise deleted messages.

Another study by Pépin and Vigliotti in 2016 [66] looked at the cryptographic side of ERTMS. They theorised a new related key attack that could break the 3DES under certain conditions. The breaking of the 3DES relied on bad cybersecurity practices and at the time of writing would have been costly (up to 47 million USD) to complete in the two year update period of keys. The study suggested moving to different algorithms such as Advanced Encryption Standard (AES). While this attack seems unlikely and the damage done would be limited, as the targeted key was KTRANS key used in key transportation, it should be considered that now computation power is available to everyone through cloud services. Therefore it would be recommended to use up-to-date cryptographic algorithms.

With the change to wireless networks the execution of electromagnetic interference (EMI) becomes easier. In 2017 Heddebaut et al. [67] looked at mitigation methods to intentional EMI from inside the train. Different antenna schemes were presented to decrease the effect of EMI to maintain better signal to noise ratio towards the base stations. However EMI will always be a problem for wireless systems as there is no way to completely remove the possibility. Moreover as discussed in sections 2.2.1-2 the EMI might not always be intentional.

While 5G offers more security options than 2G, such as base station authentication, it will still be an increase in attack surface compared to a wired system. In the ENISA 5G threat landscape 2020 it was mentioned that the 5G core moving to Internet Protocol based stack might shorten the time from a vulnerability to exploitation[68]. This threat landscape also lists the vulnerability to EMI attacks and the need for physical protection of (5G) assets.

From these observations above we can see that while some cybersecurity aspects of ERTMS/ETCS might be covered already, they are by no means free of vulnerabilities. We can also see that while FRMCS will bring many improvements, there are still inherent vulnerabilities in wireless communication.

3.4 Risk assessment

This section is focused on risk analysis. Risk analysis is a key process used in identifying and estimating risks related to the system at hand. Here the process and methods of risk analysis will be introduced.

3.4.1 Risk assessment methods used

Risk assessment is often done in three steps: identifying potential risks, impact assessment, and likelihood assessment[47]. The identification of risks can be done for example as a part of risk workshops, or identified from literature. After the risk has been identified it needs to go through impact assessment. This assessment will give us the possible consequences of the risk being realised. Then the likelihood of the risk should be assessed, giving us the chance of this risk being realised. Impact and likelihood can be assessed in either a quantitative or a qualitative way.

Risk analysis can be done either as qualitative or quantitative. Quantitative analysis is based on historical data or some other form of data that tells us how often an even occurs and how bad was it. This can be used for safety systems assuming there is enough information[41]. Qualitative risk analysis is based on the perception of the consequences and likelihood of the risk.

In cybersecurity qualitative risk analysis should be used. This is due to past events not telling us how likely the event will be in the future. A cybersecurity risk is always present and can not be counted easily in a way that would give us an hazard rate comparable to what is used in safety risks. Therefore we can only use qualitative or semiquantitative methods.[47]

The CLC/TS 50701 introduces two versions of risk assessment, initial and detailed. These tasks are done in different stages of the project and have differences for example in the evaluation matrices being used. Before the initial risk assessment a threat landscape should be created. The threat landscape will serve as the basis for the initial risk assessment. The initial risk assessment output is meant for identifying assets that share similar security needs. This is important so these assets can be placed in the proper zones.[47]

In initial risk analysis all assets in the SuC should be analysed. The process is the same as mentioned earlier, identify, assess impact, assess likelihood. It should be noted that the worst case scenario impact is used for initial risk assessment[47].

The detailed risk assessment is based on identifying threats and vulnerabilities. Then a risk acceptance principle is chosen. These principles are explicit risk evaluation, code of practice or a reference system. After a principle has been chosen the risk needs to be estimated and evaluated. As mentioned earlier cyber risks often do not have a normal likelihood, which is why they are often estimated by the exposure and vulnerabilities of the system is used instead. When this is completed, we should have a security level vector. This vector would then be used to choose countermeasures to mitigate the risks.[47]

3.4.2 Risk matrices used in this thesis

In this thesis the risk matrices used are based on the risk matrices provided in CLC/TS 50701 Annex E. There will be only matrices for initial risk assessment provided as that was the scope of this thesis. The impact is evaluated in four categories: availability, integrity (safety), confidentiality and integrity (business). The scale is from E to A, with A being the highest impact. The impact table used is presented in table 2

Table 2: Impact matrix used in this thesis.

Impact	E	D	C	B	A
Availability	typically no influence	Significant interruption of operation of a line or station or a few vehicles for a significant time	Significant interruption of operation affection a network or fleet or more than 500.000 people for a short time OR of a line or station or few vehicles for a significant time	Major interruption of operation affecting a network or a fleet or loss of service to more than 500.000 people for a significant time or of a line or station or few vehicles for a long time	Major interruption of operation affecting a network or a fleet or loss of service more than 500.000 people for a long time
Integrity (Safety)	typically no safety implications	minor safety implications, typically leading to injuries without hospitalization	safety implications, typically leading to injuries requiring hospitalization	Critical accident, typically affecting a small number of people and leading to a single fatality	Catastrophic accident, typically affecting a large number of people and leading to multiple fatalities
Confidentiality	Loss of non-security relevant data, data are not under data protection	Loss of non-security relevant data, data are not under data protection; attacker can make commercial use of the data by combing with other information	Loss of security related information, no direct access to the system is possible (physical protection), attacker cannot perform any critical safety-related commands; for example: only read access to diagnostic data are possible; loss of data under data protection law or commercially sensitive data	Loss of security related information, no direct access to the system is possible (physical protection), attacker could perform commands leading to at least critical availability, safety and business impacts.	Loss of security related information. e.g. credentials, giving direct access to the system and leading to catastrophic safety, availability or business impacts.
Integrity (Business)	Negligible business impact	Marginal business impact	Significant business impact possibly leading to substantial impact on revenue or earnings (on annual basis)	Critical business impact possibly leading to severe impact in revenue or earnings (>10 % on annual basis)	Catastrophic business impact possibly leading to bankruptcy or loss of license of operator

The likelihood matrix has two parts, exposure (EXP) and vulnerability (VUL). They are both evaluated and then the final likelihood is reached with the formula $L = EXP + VUL - 1$. The likelihood matrix is provided in table 3.

The risk acceptance matrix is a 5 by 5 matrix showing the acceptability of the risk. The levels go from low to extreme. In this model only risks within the acceptability rating low could be accepted as is. The acceptance matrix is provided in table 4.

Table 3: Likelihood matrix used in this thesis.

Likelihood	EXPOSURE	VULNERABILITY
1	Highly restricted logical or physical access for attacker, e.g. — highly restricted network and physical access, or — product or components cannot be acquired by attacker or only with high effort	— Successful attack is only possible for a small group of attackers with high hacking skills (high capabilities needed) — Vulnerability is only exploitable with high effort, and if strong technical difficulties can be solved, non-public information about inner workings of system is required — State of the art security measures to counter the threat — High chance for attacker to be traced and prosecuted
2	Restricted logical or physical access for attacker, e.g. — internal network access required, or — restricted physical access, or — product or components can be acquired by attacker with medium effort	— Successful attack is feasible for an attacker with average hacking skills (medium capabilities needed) — Vulnerability is exploitable with medium effort, requiring special technology, domain or tool knowledge — Some security measures to counter the threat — Medium chance for attacker to be traced and prosecuted
3	Easy logical or physical access for attacker, e.g. — Internet access sufficient, or — public physical access, or — attacker has access as part of daily work, operation, or maintenance activities, or — product or components can be acquired by attacker with low effort	— Successful attack is easy to perform, even for an unskilled attacker (little capabilities needed) — Vulnerability can be exploited easily with low effort, since no tools are required, or suitable attack tools freely exist. — No or only weak security measures to counter the attack caused by the threat — Low chance for attacker to be traced and prosecuted

Table 4: Risk acceptance matrix used in this thesis.

Acceptance Rating Matrix					
Impact Likelihood	E	D	C	B	A
1	Low	Low	Low	Low	Low
2	Low	Low	Low	Medium	Medium
3	Low	Low	Medium	Medium	High
4	Low	Medium	Medium	High	Extreme
5	Low	Medium	High	Extreme	Extreme

3.5 Chapter 3 summary

The railway safety standards, such as the EN 50126 series and EN 50159, are crucial in protecting humans from potential hazards, with a particular focus on reliability, availability, maintainability, and security (RAMS) throughout the system's life cycle. These standards employ a risk-based approach to reduce risks, emphasizing methods to enhance reliability and availability. The V-model outlined in EN 50126-1 serves as an important life cycle process in the railway sector. To ensure that the safety management has been adequate, the concept of independent safety assessment is introduced in the standard. EN 50126-2 deepens the requirements of safety assessment and introduces the safety integrity levels (SIL). SIL gives an estimation of how well the electronic application or function is protected from random or systematic failures. EN 50128 focuses on software-related safety, expanding the concept of SIL to software safety integrity levels (SSIL) to assess software development practices. On the other hand, EN 50129 focuses on the system safety of railway signaling systems, introducing safety-related application conditions (SRACs) and the Safety Case for comprehensive safety evaluation. However, railway security standards have been relatively lacking, with EN 50159 addressing safety-related data communication but not comprehensive cybersecurity. The recent CENELEC technical specification 50701 (CLC/TS 50701)

aims to fill this gap, presenting new concepts, including Security Levels (SL) and the security V-model, to ensure cybersecurity needs are met in the railway system.

The basis of many cybersecurity design tasks is the system under consideration (SuC) description. This description defines all the devices that are placed into security zones, and conduits that connect the zones. The zones are a critical part of detailed risk assessment and creating the requirement specification. To help with the overall design and requirement specifications of the SuC there are important design principles we can use. For railways these can be considered the most important: defense in depth, fail secure, authenticating requests, and proportionality. These are essential for building a resilient and secure railway system and making sure that the security does not interfere with safety.

The current status of cyber landscape in the railway sector has been fairly stable. We introduced some of the recent incidents of railway systems and the incidents follow the patterns that are seen in other sectors as well. What is important to note, is that the OT side of railways has not been under cyber attacks. In order to keep it that way, is why the issue of cybersecurity in the railway sector is of paramount concern.

Transitioning to the Future Railway Mobile Communication System (FRMCS) brings its own set of challenges, particularly with the adoption of wider use of wireless systems. The expanded attack surface and the risk of electromagnetic interference necessitate thorough security measures and the use of up-to-date cryptographic algorithms to mitigate potential vulnerabilities.

The risk assessment methods used in this thesis are based on the CLC/TS 50701. These offer a systematic approach to identifying and evaluating risks within the railway sector. By utilizing the provided risk matrices, We can compare risks and determine appropriate response levels to effectively manage and mitigate them.

Overall, this chapter has highlighted the complexity and critical nature of cybersecurity in the railway sector. By adhering to the outlined design principles and implementing comprehensive risk assessment methodologies, railway systems can establish robust cybersecurity strategies to safeguard against potential cyber threats and attacks. Railway sector is still behind other sectors in many cybersecurity aspects due to the systems in use having long lifecycles and cybersecurity was not the trending issue two decades ago that it is today.

4 Results

We will present the results of this thesis, a short evaluation of MCX security and the answers to our research questions. As a reminder, our research questions were:

- What are the new cybersecurity risks in 5G related to ERTMS/ETCS level 2?
- How can these risks be mitigated based on current standards?
- What do these new FRMCS related risks mean for the railway systems?

4.1 Risk assessment results

The experimental part of this thesis was to conduct initial risk identification and evaluation for the upcoming FRMCS solution as part of moving to wireless communication in ETCS level 2. This was done as a small part of the KoKoHa project. With the release of CLC/TS 50701 the aim was to follow the process from there and try to test if the cybersecurity risk analysis fits in the current FTIA safety risk format. In terms of CLC/TS 50701 this risk evaluation would be the initial risk evaluation. After the evaluation current standards were looked at to see if the risks can be mitigated by measures mentioned there. There was a total of 38 risks identified. From these 38 risks 0 were rated extreme, 3 were rated high, 18 were rated medium and 17 were rated low.

Most of the risks were identified from ENISA reports, such as the ENISA 5G threat landscape [68] and ENISA Railway Cybersecurity [10]. The 5G threat landscape lists threats towards the 5G environment while the Railway Cybersecurity report lists threat actors, assets and realised cyber attacks towards the railway sector. These have been combined with knowledge of the railway sector to select risks relevant to the railway system. It should be noted that some of the risks are relevant to all sectors, not only railways. It will be mentioned during the detailed description if the risk is railway specific.

The risks identified have been divided into groups based on roughly what type of a risk it is. These groups are software, operational, radio and physical risks. A total of 39 risks were identified. The risks are listed in tables 5, 6, 7 and 8.

In the risk tables we have the description of the risk, consequences for the risk, evaluation for likelihood and impact, and acceptance rating. Likelihood is explained further in figure 3 and impact is explained in figure 2. Acceptance rating matrix is presented in figure 4. The risks with an orange border are risks that have been realised in the railway environment.

Some of the risks did not fit the CLC/TS 50701 likelihood evaluation by exposure and vulnerability. These risks have been evaluated using the FTIA common safety method risk matrix. The common safety method scale goes from 1 to 5, where 1 is very unlikely and 5 is very likely to happen often. An example of a risk falling under this is a patch failure. A bad patch can't be evaluated by exposure and vulnerability. The reason for some of the risks not fitting the CLC/TS 50701 evaluation rises from the definition of cybersecurity to only cover malicious actions inside the standard. That is why a different evaluation method had to be used for the identified risks that are not based on malicious action.

In the risk tables the consequences are always loss of something. Many risks have more detailed consequences listed when the risks are looked at later in this section. For quick reference the tables use these terms to cover the consequences:

- **Loss of system control** means that an unauthorised user can make changes and control the system as they wish.
- **Loss of availability** means that the service or system is not available for use. An example would be that the radio network can't be used while it's being jammed.
- **Loss of information** means that information at rest or in transfer is lost or stolen. Seen as information disappearing from the system.
- **Loss of information integrity** means that we can no longer trust the information as it might have been changed.
- **Unauthorised use of the system** means that an unauthorised user can access the system and use it, but is not able to make changes or control the system.
- **Loss of system integrity** means that we can no longer trust parts of the system as they might have been tampered with.
- **Loss of software integrity** means that we lose trust in the software as it might have been changed.

4.1.1 Software related risks

Manipulation of network configuration means that an actor attempts to re-route or stop network traffic by changing our systems network settings. These changes might be done for example to the routing tables or name servers. This was identified from ENISA 5G threat landscape and was chosen to be included as there will be an increasing number of network equipment in use in ETCS. The increase of equipment comes from for example all trains needing their own routers for safety communication, no matter what technology the network is based on. The risk likelihood was evaluated as 3 because it would need at least average skills and knowledge to make meaningful edits to the configurations and the network access is restricted. This risk has low impact on safety, can have some on confidentiality and business, but the highest possible disturbance is on availability. It might lead to one track section not working or forcing it to be operated in Staff responsible mode. Therefore the impact of the risk was evaluated as D. This leads to the risk being evaluated with a risk acceptance rating of low and would not need further measures.

Software vulnerability exploitation means that an malicious actor uses holes that have not been patched yet to access the system. These holes might be for example application programming interfaces (API) that are not supposed to be public. Depending on the vulnerability and the application its located in the consequences can vary from minor to major. This risk was identified from ENISA threat landscape and was included due to new railway systems relying more heavily on software rather than hardware. Likelihood for this risk was evaluated as 2 due to needing to first enter a private network and then being able to find the vulnerability and have the skills to exploit it. This needs considerable time, effort and knowledge. The worst

Table 5: Software related risks

Software related risks		EXPOSURE	VULNERABILI	LIKELYHOOD	IMPACT	ACCEPTANCE RATING
Manipulation of network configuration	Loss of information integrity, loss of information, loss of availability	2	2	3	D	Low
Software vulnerability exploitation	Loss of availability, loss of system control, loss of information	1	2	2	B	Medium
Remote access exploitation	Loss of system integrity	2	1	2	B	Medium
Malicious code or software	Loss of availability, loss of information, loss of software integrity	2	2	3	C-B	Medium
Information leak	Loss of information	3	2	4	B	High
Authentication abuse	Loss of availability, unauthorised use of the system, loss of information	2	1	2	A	Medium
Abuse of Lawful Interception functions	Loss of information integrity, loss of information	1	1	1	B	Low
Virtualisation mechanism abuse	Loss of availability, loss of information, loss of information integrity	2	1	2	B	Medium
Manipulation of software and hardware	Loss of availability, loss of information, loss of information integrity	2	2	3	C	Medium

case is that this vulnerability can be used to change the safety software or any other critical software in the system or effect their operation. This can lead to fatalities or widespread loss of availability. That is why this risk was evaluated to have an impact of B. As such this gives the risk an acceptance rating of medium. Further measures would need to be designed and could be for example TS50701 measure SR 3.4 and the enhancement of it SR 3.4 (RE1). These mandate the integrity verification, detection and reporting of software changes. Another option would be IEC 62443 2-4 requirement SP.05.09 that locks changes to the system in normal operation.

Remote access exploitation means that a malicious actor uses our remote access methods to gain unauthorised access to the system. For example weak passwords used for remote maintenance, or session hijacking could lead to this. Remote access exploitation was identified as a risk from ENISA railway cybersecurity documentation and was chosen to be included due to the increasing availability of remote access solutions. The consequences of this risk depends considerably on what system has been gained access to. In the worst case the attacker would gain access to the safety system and could make changes to it. Thus the risk was evaluated to have impact level of B. Likelihood was evaluated as level 2, as the access is always at least from a private network and being able to achieve the highest impact you will need considerable knowledge of the system and railways. This means that the risk acceptance rating is medium. To protect the system from this type of attack there are several protective measures available. Requirements SR 2.5 and SR 2.6 control session creation, reestablishment and maximum inactivity time for a session. SR 3.8 and its enhancements cover session ID uniqueness, invalidation and integrity. For password security we can use SR 1.7 and SP.09.05 BR that both cover password strength and length requirements. Lastly we have SP.05.03 BR which says that no remote connections should be made to the safety system from out side the safety system boundary. This means that for example you could not access the safety system from a business network. Implementing SP.09.05 will make an attack considerably harder as you would need VPN or physical access to an access point to the safety system network.

Information leak was identified as a risk from ENISA railway cybersecurity documentation. This means that non-public or confidential information is accessed or downloaded by an unauthorised actor. In some cases the information might also be deleted after it has been accessed. Information leaks have occurred on railways, however they have mostly been targeted towards the IT side instead of OT. For the risk likelihood this was evaluated as 4, due to the high exposure of for example email. The impact was evaluated to be B because one of the worst cases would be stolen cryptographic keys or administrator passwords. As such the acceptance rating for this risk is high. This means that there shall be measures implemented to prevent this from happening. These measures could be such as TS50701 SR 4.1 and its enhancements, and SR 1.5 and its enhancements. In addition to these it is possible to use SR 1.1 and SR 1.2 and their enhancements to provide better authentication of users. Training of personnel is also critical to lower the likelihood of an successful phishing attack.

4.1.2 Operational risks

Information leak abuse is the next stage from the risk of information leaks. This risk was identified from the ENISA 5G threat landscape document. The information stolen in the leak can be used to execute more convincing phishing attacks or straight up compromise the system. If the stolen information is security critical, such as accounts and passwords or secret keys, the consequences of them being abused by a malicious actor can be devastating. Which is why this risk was given an impact rating of A. The likelihood was evaluated to be level 3, because you will still need access to a private network and some knowledge and skills to know how and where to use the stolen information. When these are combined the final risk acceptance rate becomes high. Measures such as stronger authentication for administrators (SR 1.1 RE 2), and protection of authentication tokens (SR 1.5) can be used to reduce the likelihood of critical information being usable by malicious actors.

Identity fraud or theft is the risk of a malicious actor forging their identity or stealing the identity of someone else. This can be used to gain access to information or areas that would not be accessible otherwise. A malicious actor being able to access those might lead to information being stolen or in some cases loss of availability. This risk was identified from ENISA threat landscape. Identity fraud as a risk was included because it opens up new opportunities for secondary attacks and it targets the weakest link in a safety or security system, the user. The likelihood was evaluated to be 4, due to access to humans often being very free. Impact was evaluated as B, as a successful attack can lead to loss of security related information. This leads to an acceptance rating of high. The measures to counter identity fraud can include multifactor authentication for users and training on information policy.

Compromised supply chain as a risk means that a supplier, which has been or is being used, is attacked and that causes issues for the system in use. This risk might also be presented as an entity part of the supply chain intentionally leaving backdoors open. This risk identified from ENISA threat documentation and was initially chosen here due to the considerable reliance on suppliers in the rail sector. After the risk analysis was already done, this risk was realised in Denmark. A supplier who created an application for the train drivers became under ransomware attack and in response shut down their service, which also took the application offline, stopping train traffic[70]. In this analysis this risk was looked at from the perspective of intentionally leaving backdoors as that would have the highest impact. To be able to be in the supply chain and leaving something behind unnoticed would require considerable skills and knowledge, therefore it was evaluated to have likelihood of 2. Considering the worst case of the safety system being compromised this way, it would be possible to cause major accidents leading to fatalities giving this risk an impact of B or possibly A if we want to err on the side of caution. Either of these would give this risk an acceptance rating of medium, thus requiring measures to be implemented. CLC/TS 50701 has very limited requirements considering supply chains, however IEC 62443-4-1 covers some aspects of supply chains. IEC 62443-4-1 sets requirements for suppliers regarding software development and guides in setting supplier requirements and how to select suppliers. There are also requirements for

Table 6: Operational risks

Operational risks		EXPOSURE	VULNERABILITY	LIKELYHOOD	IMPACT	ACCEPTANCE RATING
Network operator fraud	Loss of availability, loss of information, loss of information integrity	1	2	2	A	Medium
Information leak abuse	Loss of information, loss of information confidentiality, loss of cryptographic keys	2	2	3	A	High
Unauthorised access/intrusion to the network	Loss of system integrity, loss of information integrity	2	2	3	C	Medium
Identity fraud/theft	Loss of availability, loss of information, loss of information integrity	3	2	4	B	High
Supply chain is compromised	Loss of availability, unauthorised use of the system, loss of information	2	1	2	B-A	Medium
Nation state espionage	Loss of information integrity, loss of information	1	1	1	D	Low
Weak encryption algorithms	Loss of system control, loss of availability, loss of information, loss of information integrity			2	4	Medium
System designed with legacy equipment	Loss of availability, loss of information integrity			2	3	Low
System updates are not designed	Loss of availability, loss of information integrity			2	3	Low
Patch failure	Loss of availability, loss of information, loss of information integrity			3	3	Medium
Patching main and backup systems at the same time	Loss of availability, loss of information, loss of information integrity			2	3	Low
Accidental changes made to the system	Loss of availability, loss of information integrity			2	3	Low

integration testing that will lessen the likelihood that it would be possible to cause unwanted action. So while it might be difficult to protect against some supply chain factors, there are mitigating measures available.

Patch failure as a risk means that the patch applied to the system either causes issues on its own or introduces functionality that breaks something else. This risk was identified from ENISA threat landscapes and from this risk being assumed to be realised in Dutch railways. As this risk is often not an intentional one, the likelihood was estimated with FTIA safety risk probability. In this scale the risk was given a probability of 3, which corresponds to the risk being realised at least once during the use of the system or once every 10 years. The impact was estimated to be level 3 as assuming the down time of the Dutch GSM-R system was due to a patch, we can see it can effect a large population of people for several hours. This level 3 corresponds to level C on the CLC/TS 50701 scale. This would give the risk an acceptance rating of medium. The best measure to combat patch failures is patch management. While this does not have a particular technical requirement in CLC/TS 50701, there is a chapter for patch management and solutions provided in the standard. Here it should be noted that patch management, or patching in general, might not be a trivial thing in railways. Many of the systems are safety systems and patching a safety system will most likely require that the system go through safety approval again. This takes a long time and costs money so unless the patch is extremely critical it might never get applied. For a safety system this might be fine because the system can keep operating on the older version if it is stable. For cybersecurity however this can be a disaster. It is critical to patch vulnerabilities that are found to keep the system secure. So this introduces the issue that security patching has to be achieved in a way that it does not affect safety approval. One way to achieve this could be to have safety and security as separate layers in a way that security is on top of safety. Issues like this increase the importance of a proper patch management process that takes these items in to account. Of course also system design in this aspect is important to make these options available by keeping security and safety differentiated.

4.1.3 Radio network risks

Radio network jamming as a risk means that a malicious actor uses transmitters to send noise over the frequency band. With enough transmit power this will make it hard to recognise the actual signal from the noise. This risk was identified from ENISA 5G threat landscape and was chosen to be included because susceptibility to interference is an inherent feature of radio networks. Newer radio technologies are more resistant to this due to the better signal encoding they offer and 5G should be able to utilize frequency sensing to avoid congested frequencies. However, these will still fail with a strong enough jamming signal covering all of the available frequencies. For railways radio network jamming will cause our signalling system to not be able to communicate. This means that the train does not receive updates from the trackside and vice versa. There is a national value in ETCS that sets the time for how long the ETCS onboard unit can be without radio connection to the trackside before the train should stop. This value can be set from a few minutes to eternity. If the value

Table 7: Radio network related risks

Radio network related risks		EXPOSURE	VULNERABILITY	LIKELYHOOD	IMPACT	ACCEPTANCE RATING
Radio network jamming	Loss of availability	3	3	5	D	Low
Man in the middle/session hijacking	Loss of information integrity, loss of information	1	2	2	D	Low
DoS (denial of service)	Loss of availability	2	2	3	D	Low
Traffic tampering	Loss of information integrity, loss of information	1	1	1	C	Low
Forging signalling messages	Loss of availability, loss of information, loss of information integrity	1	1	1	A	Low
Signalling messages are captured	MAC keys can be broken with unencrypted messages and sufficient resources	1	1	1	A	Low
Forged emergency messages	Emergency messages can be used to stop traffic	1	2	2	B	Medium
Encryption algorithms are not updated	Loss of availability, unauthorised use of the system, loss of information			2	3	Low
Secret keys are not updated	Loss of availability, unauthorised use of the system, loss of information			2	4	Medium

is long enough, jamming would have to be a very large area or originate from the train cause bigger issues. Even with a shorter cut off time large scale jamming will be hard so it is over a small location and will end when the device is found. Because of these aspects, the impact of jamming was evaluated to be D. Due to the easy availability of jamming devices, the low skill needed to carry on the attack and the huge attack surface for this risk, the likelihood was evaluated to be 5. Combined this gives the risk an acceptance rating of low. This would mean that there are no further measures needed for this risk. In this risk the considered aspect has been a malicious actor, but it should be kept in mind that network jamming can also occur by accident.

Secret keys not being updated means that we keep the same secret keys in use for very long periods of time. Even with better algorithms the longer the secret is in use to more likely it is that it has been compromised. Secrets might get compromised by attacks towards systems or humans. This risk was identified in a risk workshop between railway signalling system experts. This risk was included because cybersecurity is still developing for the railways so many cybersecurity processes might not be up to standard. For this same reason the likelihood for this risk was evaluated as 2. The impact of this risk is based on the assumption that the keys would eventually be compromised and they could be used to either forge messages or control some aspects of the safety system. In these both cases it could be possible to cause accidents leading to the loss of life, therefore the impact was evaluated as 4 (comparable to impact level B). Combined these give the risk an acceptance rating of medium. This means that some measures should be taken to mitigate this risk further. One measure would be to have a key management system in place. The ERTMS specification has two key management system options defined. These are offline key management (subset-38) and online key management (subset-137). However, in baseline 3 the ERTMS key management does not suggest a maximum lifetime for keys. This is due to the ERTMS being more concerned with interoperability, so how the keys are received is more important ERTMS specifications. Therefore the owner of any secret keys should have their own key management plan in use that would cover where the keys are used, how often they are replaced and how they are replaced.

Railway specific risks

The risk of forged signalling messages rose from ENISA threat landscape and a research paper by de Ruiter et al. [65]. This risk means that someone would create and send forged signalling messages causing the train or the RBC to operate with false information. The consequences of this succeeding could be catastrophic as you could derail a train with too high speed limits or attempt to create a collision between trains. Both of these could easily lead to several fatalities. This gives the risk an impact level of A. However achieving this is very difficult. In 4G and 5G UE and base station authenticate each other so it is harder to get in between the traffic. The EURORADIO safe connection also protects the integrity and authenticity of messages giving this risk a likelihood rating of 1. Combined these give the risk an

acceptance rating of low. Even though this risk requires very high motivation and resources to become reality, it was chosen to be included because of the consequences are very severe were this to happen.

Forged emergency messages is a similar risk to forged signalling messages and was identified from the same sources. However, there is a big difference rising from the EURORADIO specification. This specification says emergency messages are sent without authentication and encryption. Emergency messages have limited functionality and are limited to emergency stop orders. This means that it would be hard to cause an accident with these, but you can cause disruption of traffic by stopping the trains. The entry into the network is hard, but once you gain access it is easier to conduct this attack than forge any other signalling messages. That is why this risk was given an likelihood rating of 2. The impact of this risk is lower than other messages, but widespread emergency stop messages can cause long delays for a wide area giving this still an impact level of B. This results in a risk acceptance rating of medium. The easiest way to fix this would be to authenticate emergency messages. You might not even need encryption as the contents are not a secret. As with other aspects in railways who sent the message and is the sender allowed to give orders are the most important aspects. With FRMCS there is the option of using MCX services which would also mitigate this risk. This is due to MCX requiring authentication from its users. So MCX would cover the gap of emergency messages not being authenticated, as they would travel over the MCX authenticated connection.

Signalling messages are captured as a risk was identified from a research paper [66] by Pépin and Vigliotti. The messages sent between ETCS entities are only authenticated and integrity protected, so they are not actually encrypted. The MAC code used in messages is based on a shared secret, KMAC, between the entities. Triple DES encryption is used to create the MAC code for the messages. Pépin and Vigliotti showed that 3DES can be broken if you have enough resources and captured messages. The consequences of the KMAC key being compromised would be that you can then act as the RBC and give orders to the train. This can lead to very severe accidents if the driver and traffic controller do not notice in time that the train is being guided to where it shouldn't go. As such this risk has been evaluated to have impact of A. However likelihood is very low as 1, due to needing millions of dollars of investments to breaking a single KMAC key (each train - RBC pair has their own key) and to gather the messages to break the key you still need to have access to a restricted network and do the attack from that restricted network. As an idea this risk was very intriguing, however it will only get harder with time. The change happens slowly in railways but eventually a stronger encryption protocol will replace 3DES. Another likely change to happen in the near future is the change from offline key management to online key management. This would allow for the keys to be changed more often, reducing the risk considerably as the time to gather the data and complete the attack will be reduced from several years to a few months.

Table 8: Physical risks

Physical risks		EXPOSURE	VULNERABILITY	LIKELYHOOD	IMPACT	ACCEPTANCE RATING
Network equipment sabotage	Loss of availability, unauthorised use of the system, loss of information	2	3	4	C	Medium
Network equipment vandalism	Loss of availability, loss of information, loss of information integrity	2	3	4	C	Medium
Terrorism	Loss of availability, loss of information, loss of information integrity	2	3	4	C	Medium
Unauthorised access to the base station	Loss of availability, loss of information, loss of information integrity	2	2	3	C	Medium
Unauthorised access to the RBC or IXL	Loss of availability, unauthorised use of the system, loss of information	2	2	3	B	Medium
System malfunction	Loss of availability			3	2	Low
Loss of power	Loss of availability			1	4	Low
Natural disasters	Loss of availability			3	2	Low

4.1.4 Physical risks

Many of the physical risks are fairly simple risks or attacks considering physically breaking them. As such only a few of them have been given a longer analysis here. All of the physical risks can be considered as general risks that are not specific to railways. However, some of these risks might be more prevalent in the rail sector due to the devices being distributed over a large geographical area.

Unauthorised access to the RBC or IXL means that an outside actor gains physical access to the devices. Having physical access to the devices means they can be tampered with. In Finland these systems will most likely be computer based

systems. As such, if there are connections left open to the device they can act as entry points for the attacker. These systems are often running special built operating systems and programs so finding vulnerabilities to exploit will require extensive knowledge and skills. So taking control of the IXL or RBC should be hard, however it could be possible for example reset the devices and cause disruption that way. In the future the IXL and RBC locations are more centralized so gaining physical access will be harder than it currently might be. This is due to reduction in equipment available next to the track in remote locations. Considering all of these factors, this risk was evaluated to have likelihood of 3. As the physical location was not yet clear, this likelihood was evaluated slightly higher than it in reality might be. The consequences of someone having physical access changes between none and catastrophic. If they are able change how the safety system works or for example do an emergency route removal, meaning a train will lose its current movement authority, it is possible to cause injuries or in worst cases fatalities. This gives us impact rating of B and a risk acceptance rating of medium. To mitigate this risk there are options such as IEC 62443 2-4 requirement SP.05.09 that locks the software of the safety system while in operation and CLC/TS 50701 SR 3.2 "malicious code protection" that requires the access points are either disabled or protected. To increase the physical security of the locations we can for example use the Finnish governmental security audition requirements called "Katakri" that lists several requirements for physical premises.

Loss of power is often raised as a risk in cybersecurity. As a cybersecurity risk loss of power could lead a system to stay in a more vulnerable state, or a system might have a vulnerability that can only be used during booting of the system. In general the biggest loss is to availability, as with no power the systems of course will not work. This risk was evaluated as a likelihood of 1 because all safety critical assets in railway sector are secured with secondary power sources. In Finland the mobile network assets have to be secured with secondary power sources due to regulation[71]. Therefore the likelihood stays low as both the main and backup power sources need to fail for this risk to realize. Impact was evaluated to be 4 (B) due to the worst possible scenario of losing functionality of an RBC so trains are unable to operate automatically in the area. This means the risk acceptance rating is low, which was to be expected as there are already strict safety requirements in place for secondary power, so they are not needed from cybersecurity side. This is still found in CLC/TS 50701 requirement SR 7.5, due to CLC/TS 50701 requirements being based on IEC 62443 3-3 standard that covers all automation systems.

4.2 Risk assessment discussion

There were two issues with the risk management as part of this work. The first issue is the initial risk assessment of CLC/TS 50701 requires impact to be estimated by the worst case scenario. This can be understood from time saving perspective but it can lead to issues of risks having higher than normal risk levels. These higher than normal risk levels can cause confusion if they are handled in the same system as safety risks. In Finland the current FTIA safety risk scale for high and extreme risks would require fast or immediate actions to be taken. This might cause unnecessary

rush in actions that would be done in detailed risk analysis anyways. Depending on the safety risk management style, it seems to be a good idea to keep the security and safety risks separated until the detailed risk assessment is done.

The second issue was directly related to this specific risk analysis. There was no SuC available for the risk analysis. While threat landscapes were used, the lack of SuC left the risk analysis as too high level. Creating the SuC was also out of scope for this thesis. However this issue made it so that the risk registry can be published, as it only contains higher level risks that are present in already public materials.

To answer the research question of new risks in 5G related to ETCS level 2 the risks are related to the ability to interfere with the communication media. This is not a 5G specific risk though, as GSM-R will also suffer from this. So in reality the only new risks will be related to the new 5G core. The 5G core risks looked at consisted of the abuse of virtualisation. This risk was in the medium risk level due to the 5G core being a restricted system and requiring significant knowledge of the subject. Outside of this there might be new risks for Finland moving from level NTC to level 2 or higher, but many of these risks are already present in the GSM-R system already in use in Europe.

The second research question was about mitigating these risks based on current standards. We have shown a few examples of mitigation techniques related to risks identified. Following the design principles in CLC/TS 50701 and the requirements for different security levels mitigate many of the risks. ISO 27000 series can also be used to cover the management side. Some of the application side security issues should be covered by EN 50129, due to the strict requirements for software with safety integrity levels.

The third question was about what do these risks mean for the railway systems. Based on the reports[10, 52] shown of railway cybersecurity maturity it is clear that there is work to be done. Cybersecurity practices should be implemented to all new and ongoing projects to make sure that in the future the railway systems stay secure. This means that all railway sector stakeholders need to work towards a secure railway. A lot of this might fall on the suppliers providing sufficient systems but the role of infrastructure managers including cybersecurity requirements from CLC/TS 50701 or EN IEC/IEC 62443 series can not be understated.

The question of MCX end to end security was raised by Mr Lyly in one of the interviews. So while it was not one of the original research questions, this question was also looked at. The MCX common security requirements seem in line with CLC/TS 50701, while it is not a communications cybersecurity standard, the good practices should not differ much.

To specifically answer the end-to-end security the 4G MCX security defined in ETSI TS 133 130[72], the end-to-end security is done by a key management (KMS) service using the identities of the mission critical users to start a secured connection. While it is not the same as public key encryption it seems to work in a similar way. There are security parameters sent during the authentication process and those parameters are used also in the connection setup by the KMS. With these findings the end-to-end security of MCX operations seems to be in good shape. However as this method might be based on for example usernames and passwords, setting these

up and making sure that the applications that can be used are secure becomes the critical point of ensuring system security.

5 Conclusions

This thesis looked at the Future Railway Mobile Communications System and what risks it might bring to the railway systems. We found out that while there are new risks introduced, many of the risks are already present in GSM-R systems also. This means that several of the risks are introduced by moving to a wireless communication system instead of the technology used for the system.

There were a total of 38 risks identified with most of the risks being evaluated as medium or low rating. There were three risks that had a rating of high and no extreme ratings were identified. Some of the risks were out of scope of the CLC/TS 50701 methodology so they were evaluated by methods used for safety risk assessment. Two of the high risks were related to data breaches, and the third one was about identity theft. The common nominator between these risks was the inherent involvement of humans. As can be seen in the ENISA 2021 threat landscape phishing remains one of the most common methods of entering a system[69]. This is why these risks were given a higher likelihood and when the impact is considered as the worst case scenario, the risk level is increased. The amount of medium risks, over half of the risks, shows that the upcoming railway communication system is not fully secure.

The risks in the low estimation held some of the most interesting ones. The insertion of emergency messages discussed in [65] ended up with a low risk rating due to the problematic nature of getting between the communicating RBC and OBU. The risk likelihood was further reduced due to the FRMCS having MCX which requires authentication, so while EURORADIO does not require authentication MCX would cover it. The risk level of EMI also ended up being low. While EMI had a high likelihood, the impact of EMI is considered low. You can stop trains from communicating, which leads to them stopping at the end of their movement authority. So while it can be a nuisance, the effects were considered local and short term.

What should be noted of these risks is that all of them have mitigating measures available. These measures can be found in current standards such as CLC/TS 50701, IEC 62443 series and ISO 27000 series. The measures for most risks would be technical requirements for the system or components, however some risks can only be mitigated by cybersecurity processes. As we can see that there are measures available it will be possible to make the jump and increase the cybersecurity of railways. It is a long process that requires suppliers to start implementing security options in their solutions now. This also means that system owners need to start pushing the bar higher to show interest in cybersecurity and motivate the suppliers to act.

One way to help this transition would be to have a harmonised standard for cybersecurity in railways. Currently for railway safety in Europe the EN 50126, EN 50128, EN 50129 and EN 50159 are considered harmonised standards meaning that all railway actors have to follow them. While it is still uncertain if it will become a harmonised standard there is IEC 63452 standard coming that is the next step from CLC/TS 50701. This standard is currently in the Committee Draft stage and is expected to be ready during summer 2025. IEC 63452 has the possibility of becoming the harmonised standard for cybersecurity. While railway stakeholders are of course

already doing some cybersecurity actions, a harmonised standard would ensure that all stakeholders have at least the same base level of security.

The CLC/TS 50701 brought the OT standard IEC 62443 series to the railway sector. This specification is a good step towards railway cybersecurity and it held many useful concepts such as the design principles, security levels and handling of legacy equipment. However, there are some issues also present. The OT management plan introduced is not properly gone over and there is no proper information on the operational stage for cybersecurity. It could also benefit from a EN 50126 style independent assessment for cybersecurity. While CLC/TS 50701 can be used right now, it might not reach harmonised standard level.

To help in up-keeping cybersecurity it would be beneficial to separate security and safety. There is often a long process for safety approval and once that is accepted any changes to safety can mean that it needs to go through the approval process again. Before cybersecurity this is not an issue as you might not need to update the system until you are buying a new one. However a key point of cybersecurity is that you need to be able to update it to close vulnerabilities or update firewalls to recognise newest threats. Therefore security should be built as an extra layer outside of safety, so that security can be updated without needing new safety approval process.

During this work it was also discovered that handling safety and security risks in the same system might cause confusion due to higher risk levels than expected. This is only relevant to the initial risk assessment phase described in CLC/TS 50701, but it should be kept in mind. Depending on the actions that the risk acceptance matrix should lead to, it might be beneficial to keep the initial risk assessment and safety risks separated.

References

[1] Statistics Explained. "Railway passenger transport statistics - quarterly and annual data" Eurostat. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Railway_passenger_transport_statistics_-_quarterly_and_annual_data#Rail_passenger_transport_performance_continued_to_increase_in_2019 (accessed Nov. 10, 2022).

[2] European Council. Official Journal L 235. (1996, July 23). *Council Directive 96/48/EC of 23 July 1996 on the interoperabiliti of the trans-European high-speed rail system.* [Online] Available: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0048:EN:HTML

[3] Data Browser. "Goods transported (detailed reporting only) - Quarterly data." Eurostat. https://ec.europa.eu/eurostat/databrowser/view/rail_go_quartal/default/table?lang=en (accessed Aug. 3, 2021)

[4] European Commission. "ETCS levels and modes." Mobility and Transport. https://ec.europa.eu/transport/modes/rail/ertms/etcs-levels-and-modes_en (accessed Dec. 12, 2021)

[5] European Union Agency for Railways, "ERTMS/ETCS System Requirements Specification, SUBSET-026-2 v3.6.0", May 2016. [Online]. Available: https://www.era.europa.eu/era-older/archived-set-specifications-3-etcs-b3-r2-gsm-r-b1

[6] EEIG ERTMS User Group, "Hybrid ERTMS/ETCS Level 3 (v1D)", 2020. [Online]. Available: https://ertms.be/wp-content/uploads/2023/06/16E0421F_HTD.pdf

[7] UIC Rail System Department, "FRMCS and 5G for rail: challenges, achievements and opportunities," Dec. 2020. [Online]. Available: https://uic.org/IMG/pdf/brochure_frmcs_v2_web.pdf

[8] K. Orbele, "Making 5G A Rail Reality," *Railway Age*, vol. 221, no. 5, pp. 26-28, May 2020.

[9] J. Pylvänäinen et al. "Digirata-valmisteluvaiheen loppuraportti," Ministry of Transport and Communications, Finland, June 2021. [Online]. Available: https://digirata.fi/wp-content/uploads/2021/07/Digirata-valmisteluvaiheen-loppuraportti_FINAL.pdf

[10] D. Liveri, M. Theocharidou and R. Naydenov, "ENISA Report - Railway Cybersecurity," ENISA, Nov. 13, 2020. [Online]. Available: https://www.enisa.europa.eu/publications/railway-cybersecurity

[11] R. Chen, W. -X. Long, G. Mao and C. Li, "Development Trends of Mobile Communication Systems for Railways," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3131-3141, Fourthquarter 2018, doi: 10.1109/COMST.2018.2859347.

[12] NIS Cooperation Group, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures," European Commission, Jan. 23, 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[13] J. Wu and P. Fan, "A Survey on High Mobility Wireless Communications: Challenges, Opportunities and Solutions," in IEEE Access, vol. 4, pp. 450-476, 2016, doi: 10.1109/ACCESS.2016.2518085.

[14] "COMMISSION IMPLEMENTING REGULATION (EU) 2017/6 on the European Rail Traffic Management System European deployment plan" (2017) *Official Journal* L3 p. 6-28

[15] M. Ruete, "1st Work Plan of the European Coordinator for ERTMS," European Commission, May 2020. [Online]. Available: https://transport.ec.europa.eu/1st-work-plan-european-coordinator-ertms-matthias-ruete_en

[16] European Union Agency for Railways, "ERTMS/ETCS Functional Requirements Specification," June 21, 2007. [Online]. Available: https://www.era.europa.eu/system/files/2023-01/sos1_index001_-_era_ertms_003204_v500.pdf

[17] Aki Härkönen et al. "ERTMS/ETCS-liikennöinnin toimintaperiaatteet," Finnish Transport Infrastructure Agency, Feb 1, 2019. [Online]. Available: https://ava.vaylapilvi.fi/ava/Julkaisut/Vaylavirasto/vo_2019-08_ertms-etcs_liikennoinnin_web.pdf

[18] European Commission. "What are the benefits." Transport and Mobility. https://transport.ec.europa.eu/transport-modes/rail/ertms/what-are-benefits_en (accessed Sept. 24, 2022).

[19] GSM-R Functional Group, "GSM-R Functional Requirements Specification," International Union of Railways, Dec. 21, 2015. [Online]. Available: https://www.era.europa.eu/system/files/2023-01/sos3_index032_-_eirene_frs_v800.pdf

[20] T. Anttila et al. "Ratatekniset ohjeet (RATO) osa 10 Junien kulunvalvonta JKV," Finnish Transport Infrastructure Agency, July 1, 2022. [Online]. Available: https://ava.vaylapilvi.fi/ava/Julkaisut/Vaylavirasto/vo_2021-40_rato10_web.pdf

[21] J. Pylvänäinen et al. "Digirata-selvityksen loppuraportti," Ministry of Transport and Communications, Finland, Apr. 2, 2020. [Online]. Available: https://digirata.fi/wp-content/uploads/2020/04/Digirata_loppuraportti_02042020.pdf

[22] R. He et al., "High-Speed Railway Communications: From GSM-R to LTE-R," in IEEE Vehicular Technology Magazine, vol. 11, no. 3, pp. 49-58, Sept. 2016, doi: 10.1109/MVT.2016.2564446.

[23] P. Winter, Ed., "Railway communication: the GSM-R developments," in *Compendium on ERTMS,* B. Guiot, Ed., Hamburg, Germany:Eurail Press, 2009.

[24] P. Sun, J. Ding, S. Lin, D. Fei and W. Wang, "Research on Co-channel Interference between LTE-R and GSM-R Wireless Networks in 900MHz," 2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting, Montreal, QC, Canada, 2020, pp. 1213-1214, doi: 10.1109/IEEECONF35879.2020.9329546.

[25] Finland, Traficom. (Jan. 12, 2023). *Regulation 4 AD / 2023M, Radio frequency regulation.* Accessed: Mar. 3, 2023. [Online]. Available: https://www.traficom.fi/sites/default/files/media/regulation/Radio%20frequency%20regulation%204AD3023M.pdf

[26] FMS Telecom On-Board Architecture Workgroup, "FRMCS Telecom On-Board System - Architecture Migration Scenarios," International Union of Railways, Apr. 15, 2020. [Online]. Available: https://uic.org/IMG/pdf/frmcs_telecom_on-board_system_-architecture_migration_scenarios-toba7540-1.0.0.pdf

[27] European Union Agency for Railways, "EuroRadio FIS," Dec. 17, 2015. [Online]. Available: https://www.era.europa.eu/system/files/2023-01/sos3_index010_-_subset-037_v320.pdf

[28] FRMCS Functional Working Group, "Future Railway Mobile Communication System User Requirements Specification," International Union of Railways, Feb. 24, 2023. [Online]. Available: https://uic.org/IMG/pdf/frmcs_user_requirements_specification-fu_7100-v5.1_0.pdf

[29] B. Sun, J. Ding, S. Lin, W. Wang, Q. Chen and Z. Zhong, "Comparison Analysis on Feasible Solutions for LTE Based Next-Generation Railway Mobile Communication System," *ZTE Communications,* vol. 17, no. 1, pp 56-62, Mar. 2019, doi: 10.12142/ZTECOM.201901009.

[30] G. Noh, B. Hui and I. Kim, "High Speed Train Communications in 5G: Design Elements to Mitigate the Impact of Very High Mobility," in IEEE Wireless Communications, vol. 27, no. 6, pp. 98-106, December 2020, doi: 10.1109/MWC.001.2000034.

[31] B. Ai, A. F. Molisch, M. Rupp and Z. -D. Zhong, "5G Key Technologies for Smart Railways," in Proceedings of the IEEE, vol. 108, no. 6, pp. 856-893, June 2020, doi: 10.1109/JPROC.2020.2988595.

[32] P. T. Dat, A. Kanno, K. Inagaki, F. Rottenberg, N. Yamamoto and T. Kawanishi, "High-Speed and Uninterrupted Communication for High-Speed Trains by Ultrafast WDM Fiber–Wireless Backhaul System," in Journal of Lightwave Technology, vol. 37, no. 1, pp. 205-217, 1 Jan.1, 2019, doi: 10.1109/JLT.2018.2885548.

[33] K. S. Solanki and K. Chouhan, "Implementation of High Speed Railway Mobile Communication System," *International Journal on Recent and Innovation Trends in Computing and Communication,* vol. 5, issue 8, pp. 41-44, Aug. 2017.

[34] S. Writer. "World's first LTE-Railway service goes live on new high-speed train line in Korea." cioafrica.com. https://cioafrica.co/worlds-first-lte-railway-service-goes-live-new-high-speed-train-line-korea/ (accessed Mar. 4, 2023).

[35] Digirata. "EMMA-vaunun testausmatka on viety loppuun: Mittaustulosten perusteella kaupalliset verkkoyhteydet tarpeeksi kattavia junaliikenteen viestintään." digirata.fi. https://digirata.fi/emma-vaunun-testausmatka-on-viety-loppuun-mittaustulosten-perusteella-kaupalliset-verkkoyhteydet-tarpeeksi-kattavia-junaliikenteen-viestintaan/ (accessed Mar. 4, 2023).

[36] Technical Specification Group Services and System Aspects, "Study on Future Railway Mobile Communication System," 3GPP, TS 22.889 V17.4.0, Mar. 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3162

[37] Rail Telecommunications, "FRMCS; Study on system architecture," ETSI, TR 103.459 v.1.2.1, Aug. 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103400_103499/103459/01.02.01_60/tr_103459v010201p.pdf

[38] *Mission Critical Services Common Requirements (MCCoRe),* 3GPP TS 22.280 V18.2.0, 3rd Generation Partnership Project, Jun. 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3017

[39] *Functional Architecture and information flows to support Mission Critical Data (MCData),* ETSI TS 123.282 v16.8.0, European Telecommunications Standards Institute, Jan. 2021. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123200_123299/123282/16.08.00_60/ts_123282v160800p.pdf

[40] Finnish Transport Infrastructure Agency. "List of railway guidance." vayla.fi https://ava.vaylapilvi.fi/ava/Julkaisut/OL/rautatieohjeet.pdf (accessed Mar. 5, 2023).

[41] *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process,* EN 50126-1, Oct. 2017.

[42] *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety,* EN 50126-2, Oct. 2017.

[43] *Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 3: Guide to the application of EN 50126-1 for rolling stock RAM,* CLC/TR 50126-3, July 2008.

[44] *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems,* EN 50128, June 2011.

[45] *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling,* EN 50129, Nov. 2018.

[46] *Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems,* EN 50159 (+ A1), Sep. 2010 (Feb. 2020).

[47] *Railway applications - Cybersecurity,* CLC/TS 50701, July 2021.

[48] K. Helmut and C. Schlehuber, "Zoning and Conduits for Railways," ENISA, Feb. 2022. [Online]. Available: https://er.isacs.eu/sites/default/files/flmngr/publications/Zoning%20and%20Conduits%20for%20Railways%20-%20Security%20Architecture%20(2).pdf

[49] *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design,* IEC 62443-3-2, June 2020.

[50] M. A. Wischy and C. Horn, "Deliverable D8.2-3b Protection Profile - Trackside components," X2Rail-3, Dec. 2020. [Online]. Available: https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3

[51] M. A. Wischy and C. Horn, "Deliverable D8.2-3c Protection profile – On-board components," X2Rail-3, Dec. 2020. [Online]. Available: https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3

[52] R. Kour and R. Karim, "Cybersecurity workforce in railway: its maturity and awareness," *Journal of Quality in Maintenance Engineering,* vol. 27 no. 3, pp. 453-464, July 2021, doi: 10.1108/JQME-07-2020-0059.

[53] BBC News. "Ukraine power cut 'was cyber attack'." BBC.com. https://www.bbc.com/news/technology-38573074 (accessed Mar. 10, 2023).

[54] T. Chesire. "Four Cyber Attacks On UK Railways In A Year." Sky News.https://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558 (accessed Mar. 10, 2023).

[55] J. Nasr. "German rail operator affected by global cyber attack." Reuters.com https://www.reuters.com/article/us-cyber-attack-germany-rail-idUSKBN1890DM (accessed Mar. 10, 2023).

[56] B. Barth. "DDoS attacks delay trains, stymie transportation services in Sweden." SCmagazine.com. https://www.scmagazine.com/news/ddos-attacks-delay-trains-stymie-transportation-services-in-sweden (accessed Mar. 10, 2023).

[57] The Copenhagen Post. "Hackers target Danish train service over the weekend." CPHPost.dk. http://cphpost.dk/news/hackers-target-danish-train-service-over-the-weekend.html (accessed Mar. 10, 2023).

[58] Z. Kleinmann. "Rail station wi-fi provider exposed traveller data." BBC.com https://www.bbc.com/news/technology-51682280 (accessed Mar. 10, 2023).

[59] M. Winder. "Cyber-attack against Stadler IT network." StadlerRail.com. https://www.stadlerrail.com/media/pdf/2020_0507_media%20release_cyber-attack_en.pdf (accessed Mar. 10, 2023).

[60] D. Burroughs. "Adif hit by cyberattack." railjournal.com. https://www.railjournal.com/technology/adif-hit-by-cyberattack/ (accessed Mar. 10, 2023).

[61] Q. Vosman. "GSM-R failure cripples Dutch network." railjournal.com. https://www.railjournal.com/passenger/main-line/gsm-r-failure-cripples-dutch-network/ (accessed Mar. 10, 2023).

[62] A. Roth. "'Cyberpartisans' hack Belarusian railway to disrupt Russian buildup." TheGuardian.com. https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup (accessed Mar. 10, 2023).

[63] A. Smith. "Hackers attack train network to stop Putin moving troops from Russia to Ukraine." Independent.co.uk. https://www.independent.co.uk/tech/hackers-attack-train-putin-troops-russia-ukraine-b2024907.html (accessed Mar. 10, 2023).

[64] Y. Sun and H. Song, eds. *Secure and Trustworthy Transportation Cyber-Physical Systems.* Singapore: Springer Singapore, 2017.

[65] A Formal Security Analysis of ERTMS Train to Trackside Protocols Joeri de Ruiter, Richard J. Thomas(B), and Tom Chothia School of Computer Science, University of Birmingham, Birmingham, UK Springer International Publishing Switzerland 2016 T. Lecomte et al. (Eds.): RSSRail 2016, LNCS 9707, pp. 53–68, 2016. DOI: 10.1007/978-3-319-33951-1 4

[66] Risk Assessment of the 3Desin ERTMS Florent Pépin and Maria Grazia Vigliotti(B) RSSB, 1 South Place, London EC2M, UK Springer International Publishing Switzerland 2016 T. Lecomte et al. (Eds.): RSSRail 2016, LNCS 9707, pp. 79–92, 2016. DOI: 10.1007/978-3-319-33951-1 6

[67] M. Heddebaut, V. Deniau, J. Rioult and C. Gransart, "Mitigation Techniques to Reduce the Vulnerability of Railway Signaling to Radiated Intentional EMI Emitted From a Train," in IEEE Transactions on Electromagnetic Compatibility, vol. 59, no. 3, pp. 845-852, June 2017, doi: 10.1109/TEMC.2016.2635259.

[68] European Union Agency for Cybersecurity, "Enisa 5G Threat Landscape for 5G Networks," Dec. 2020. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

[69] European Union Agency for Cybersecurity, "ENISA Threat Landscape 2021," Oct. 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[70] G. Van de Ven. "How a supply-chain cyberattack paralyzed the Danish railway." Conquer-your-risk.com. https://www.conquer-your-risk.com/2022/12/06/how-a-supply-chain-cyberattack-paralyzed-the-danish-railway/ (accessed Mar. 15 2023)

[71] Finland, Traficom. *Regulation on resilience of communications networks and services and of synchronisation of communications networks.* Accessed: Nov. 20, 2023. [Online]. Available:https://www.finlex.fi/fi/viranomaiset/normi/480001/47143

[72] *Security of the Mission Critical (MC) service,* ETSI TS 133 180 v17.7.0, European Telecommunications Standards Institute, Sep. 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133100_133199/133180/17.07.00_60/ts_133180v170700p.pdf