Tampere University

Juha Manninen

IT AND OT CYBERSECURITY PRACTISES FOR DIGIRAIL

Master of Science Thesis
Faculty of Information Technology and Communication Sciences
Matti Monnonen
Marko Helenius
April 2022

ABSTRACT

Juha Manninen: IT and OT cybersecurity practises for Digirail
Master of Science Thesis
Tampere University
Master's Programme in Information Technology
April 2022

With digitalisation, the importance and relevance of cybersecurity is also increasing for industrial systems and environments. Railway environments are also going through a digitalisation and in Finland this is happening with the Digirail project. Since cybersecurity is a quite new topic for railways and there is not that much guidance about the topic, it is useful to research the topic and produce that needed guidance. This thesis aims to find the best parts of OT and IT cybersecurity practises that could be used for Digirail by using cybersecurity standards as guideline.

The thesis divides into two parts from which the background is the first. The background part focuses on the Digirail project from more overall level and also gives an overview for cybersecurity in railway environments. IT and OT systems and their differences and aspects are also introduced in the background part. The other part of the thesis focuses on the actual research that contains the interviews and studying the three cybersecurity standards.

As said before the research and the thesis focused on three cybersecurity standards. The first standard is TS50701 which is a cybersecurity standard specifically for railway environments released by CENELEC in 2021. It is also the standard that was the main focus point for this research.

Other standards that were studied are IEC 62443 and ISO/IEC 27001. The IEC 62443 is a general cybersecurity standard for OT environments and the TS50701 standard is based on it. The ISO/IEC 27001 on the other hand is more for IT focused systems and it gives guidance for information security management.

The thesis also included few interviews for different Digirail personnel. The point was to get better perspective for digirail environment overall and better understanding of cybersecurity for this kind of environment. There were four interviews in total, and they turned out be somewhat challenging but at the same time beneficial for this thesis and also interesting. The challenges with the interviews derived from the different backgrounds of the interviewees and how difficult it was to adapt the interview according to that.

The research showed that the TS50701 standards is a quite well-made standard and it contains a lot of relevant and important cybersecurity guidance that could be used for Digirail. It is derived from the IEC 62443 standard series but it also gives railway specific additional guidance. There are topics however that are not covered well like incident management which could be studied further.

The ISO/IEC 27001 and IEC 62443 give guidance that could be used as an additional information to support the TS50701. There are parts that overlap between the standards and there is a table that shows the most relevant parts of each standard at the end of this thesis. A bit of comparing is be done after the studying the standards.

This thesis gives guidance for coherent cybersecurity management for Digirail that covers both IT and OT side. Other topics that were not included in this thesis could be studied also from the standards. The next steps could be trying to implement the guidelines form the standards into practise.

Keywords: Digirail, Cybersecurity, Cybersecurity standard, TS50701, ISO/IEC 27001, IEC 62443

TIIVISTELMÄ

Juha Manninen: Digiradan IT ja OT kyberturvallisuus
Diplomityö
Tampereen yliopisto
Tietotekniikan DI-ohjelma
Huhtikuu 2022

Digitalisaation myötä myös raideliikenne on muuttumassa ja kyberturvallisuuden merkitys kasvamassa. Suomessa meneillä olevalla Digirata-hankkeella kehitetään raideliikenteen digitalisaatiota ja sen myötä myöskin kyberturvallisuuden merkitys kasvaa. Koska kyberturvallisuus on uusi asia raideliikenteessä, eikä valmiita ohjeistuksia ole vielä paljon, on tärkeää kehittää uusia ja yhtenäisiä ohjeistuksia. Tämän diplomityön tavoitteena on löytää parhaat IT ja OT kyberturvallisuuden keinot, joita voitaisiin hyödyntää Digiradassa.

Tämä diplomityö koostuu kahdesta osasta, joista ensimmäinen on taustoitusta työlle. Taustoitus luvussa käsitellään Digirata-hanketta yleisesti, kyberturvallisuutta rautatiemaailmassa, sekä IT ja OT-ympäristöjä ja niiden eroavaisuuksia. Toinen osa diplomityöstä on itse tutkimusosio, joka sisältää haastattelut sekä kolmen kyberturvallisuuden standardin tutkimisen.

Kuten aiemmin mainittiin, tässä työssä tutkitaan kolmea eri kyberturvallisuuden standardia. TS50701 on uusi CENELECin vuonna 2021 julkaisema raideliikenteelle tarkoitettu kyberturvallisuuden standardi, joka oli myöskin tässä diplomityössä tärkein ja päällimmäinen tutkimuksen kohde.

TS50701:n lisäksi tutkittavana olivat standardit ISO/IEC 27001 ja IEC 62443. Ne ovat yleisempiä kyberturvallisuuden standardeja, joista ISO/IEC 27001 on enemmän IT-ympäristöön suunnattu ja IEC 62443 puolestaan OT-ympäristöön.

Kuten mainittiin, työssä myös suoritettiin haastatteluita Digiradan kanssa työskenteleville henkilöille. Tarkoituksena oli kartoittaa Digiradan kokonaiskuvaa ja arkkitehtuuria ja kasvattaa ymmärrystä kyberturvallisuudesta Digiradan kaltaisessa ympäristössä. Haastattelut osoittautuivat hieman haasteellisiksi, mutta myös samalla hyödyllisiksi ja kiinnostavaksi. Haasteet johtuivat haastateltavien eri taustoista, ja siitä miten oli hankalaa sovittaa haastattelua niiden mukaan.

Standardien tutkimisen perusteella havaittiin, että TS50701 on kattava standardi, joka sisältää paljon oleellista ohjeistusta, jota voidaan myös Digiradan tarpeita varten hyödyntää.TS50701 perustuu IEC 62243-standardisarjaan ja siinä onkin useita viittauksia siihen. Joitakin tärkeitä IT/OT-ympäristöön puuttuvia asioita, kuten poikkeustilanteiden hallinta standardista kuitenkin puuttuu. Tämä onkin esimerkki siitä, mitä voisi tutkia vielä tarkemmin.

IEC 62443 ja ISO/IEC 27001 sisältävät ohjeistuksia näistä aiheista myös ja niitä voisi myös tarvittaessa soveltaa Digiradan ohjeistuksiin täydentämään TS50701 standardin ohjeistusta. IEC 62443 ja ISO/IEC 27001 standardit menevätkin jonkin verran päällekkäin TS50501 standardin ja työn lopussa on taulukko, jossa on jokaisen standardin oleellisimmat osat merkittynä.

Tässä diplomityössä etsittiin yhtenäistä IT ja OT-puolet kattavaa kyberturvallisuuden ohjeistusta Digiradalle standardeja hyödyntäen. Muitakin asioita, joita tässä diplomityössä ei tarkasteltu voisi tutkia standardeista. Eräänä jatkokehityskohteena voisi olla selvittää, miten standardeista löytyneitä ohjeistuksia voidaan hyödyntää käytännössä.

Avainsanat: Digirata, Kyberturvallisuus, Kyberturvallisuusstandardi, TS50701, ISO/IEC 27001, IEC 62443

PREFACE

This master's thesis was done while I was working at Proxion. The work was done for a customer as a research project and as a part of the Digirail project.

I would like to thank the personnel from Proxion who helped with finding the topic and with the process. I would like also to thank the customer for this opportunity and for feedback on the work and I would like to thank the personnel who took part in the interviews. Finally, I would like thank my university instructor for also helping with the process.

Tampere, 29 April 2022

Juha Manninen

CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

5G	Fifth generation technology standard for cellular networks
AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
ATO	Automatic Train Operation
ATP	Automatic Train Protection
CENELEC	European Committee For Electrotechnical Standardization
CIA	Confidentiality, Integrity and Availability model
DDos	Distributed Denial of Service
DES	Data Encryption Standard
Digirail	English title for the Digirata project
DMI	Driver Machine Interface
DMZ	Demilitarized zone
DoS	Denial of Service
ERTMS	European Rail Traffic Management System
ETCS	European Traffic Control System
EVC	European Vital Computer
FR	Foundational Requirement
FRMCS	Future Railway Mobile Communication System
GSM-R	Global System for Mobile Communications – Railway
IACS	Industrial Automated Control System
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization of Standardization
IT	Information Technology
KMC	Key Management Centre
LEU	Lineside Electronic Unit
MAC	Message Authentication Code
MITM	Man-In-The-Middle
OBU	Onboard unit
OT	Operational Technology
RAMS	Reliability Availability Maintainability Safety
RBC	Radio Block Centre
SCADA	Supervisory Control And Data Acquisition
SecRAC	Security-related application condition
SHA	Secure Hash Algorithm
SIL	Security Integrity Level
SR	System Requirement
SuC	System under Consideration
TIMS	Train Integrity Monitoring System
ZCR	Zone and Conduit Requirements

1. INTRODUCTION

Digitalization is affecting industries all over the world and the railway industry is also going through changes towards more digitalized environment. Old railway systems are starting to get outdated and newer more efficient systems are needed to replace them. In Finland the railway digitalization is happening via the Digirail project. The Digirail project is a long and large project that is supposed to last several years. It has experts working on several different topics and working groups. The project aims to replace older railway systems with newer ones that are up to date with European standards.

With digitalization comes more connectivity and the importance of cybersecurity rises drastically. Railway environment has information technology (IT) and operational technology (OT) systems that are going to get converged together. Connecting OT systems into an IT network is not something that should be done without proper and careful planning and consideration. IT and OT are different environments and specially from the perspective of cybersecurity. OT systems have been isolated for a long time so connecting them with IT could expose the whole system to its weaknesses if done carelessly.

Cybersecurity in general is a new topic for railways and with digitalization comes new threats. Railway industry has already been a target for some cyberattacks, but the numbers are still quite low. This could change in the future and more hackers could target railway with their cyberattacks.

Finding out the best of both IT and OT and combining them is a way towards the connected system. The new cybersecurity standard TS50701 that is made by CENELEC gives guidance on how cyber security should be handled in railway environment. Other standards such as ISO/IEC 27001 and IEC 62443 also have relevant guidance for cybersecurity.

Railways are in a need of a comprehensive cybersecurity management approach that covers both IT and OT. This thesis focuses on the IT and OT systems and the best cybersecurity practises that are used for managing these systems in the Digirail context. This thesis aims to find the answers for these questions.

1. How well does the TS50701 standard include IT and OT cybersecurity best practises for Digirail?

2. What cybersecurity practises can be found from ISO/IEC 27001 and IEC 62443 standards to complement the TS50701 standard?

3. Are there any points for further research about IT and OT cybersecurity practises for Digirail?

TS50701 standard is covered in the chapter 4 of this thesis whereas standards ISO/IEC 27001 and IEC 62443 are covered in chapter 5 of the thesis. In chapter 6 the standards and their contents are then reviewed in the context of Digirail.

2. BACKGROUND

This chapter covers the overall background information for the scope of this thesis and research. The point is set up the research part that of the thesis. Background covers the basics of the Digirail project and all the most relevant subtopics that are related to it like European rail traffic management system (ERTMS), Future railway mobile communication system (FRMCS) and different interfaces within the overall architecture.

Railway cybersecurity is a topic that is covered from a generic overall point of view on this chapter since it is a relevant topic for this thesis. This chapter includes going through some examples of cyberattacks and scenarios that have happened or that could happen in railway environments. The point is to give a better understanding of how cybersecurity affects or how it could affect railway environments.

Since this thesis focuses on IT and OT system best practises it is important to have background information about IT and OT. This chapter also covers the basic aspects of IT and OT environments and their differences in terms of cybersecurity.

2.1 The Digirail project

The Finnish railway systems are going through a transformation. The current Finnish automatic train protection (ATP) is nearing the end of its lifecycle and it is no longer actively developed. The document from Finnish ministry of transport and communications [36] mentions that since Finland is part of Europe's train track area the Finnish tracks are going to be implemented with ERTMS. The Digirail project aims to replace the current system before the end of its lifecycle, and it is also an opportunity to modernize and digitalize the railway systems in Finland. This includes systems and devices like traffic control and track safety equipment.

The document [36] mentions that the Digirail project is divided into different phases that are the research phase, preparatory phase, the development and verification phase and the execution phase. At the time of writing this thesis the current phase is the development and verification phase.

2.2 ERTMS

Finnish ministry of transport and communications published a document which describes ERTMS [1]. ERTMS is a new standard for European automatic train protection and since

ERTMS will be the general standard in Europe it means that the same train unit could drive through different countries in Europe if those countries are using ERTMS. ERTMS itself consists of different parts from which European train control system (ETCS) is the signalling system and component used for controlling ERTMS. FRMCS will be the new radio communication standard for railways, and it will be based on fifth generation mobile network (5G) technology. European traffic control system ETCS will replace the old legacy train protection systems. ERTMS/ETCS has different levels which are shown in Figure 1 which is based on the same document [1].

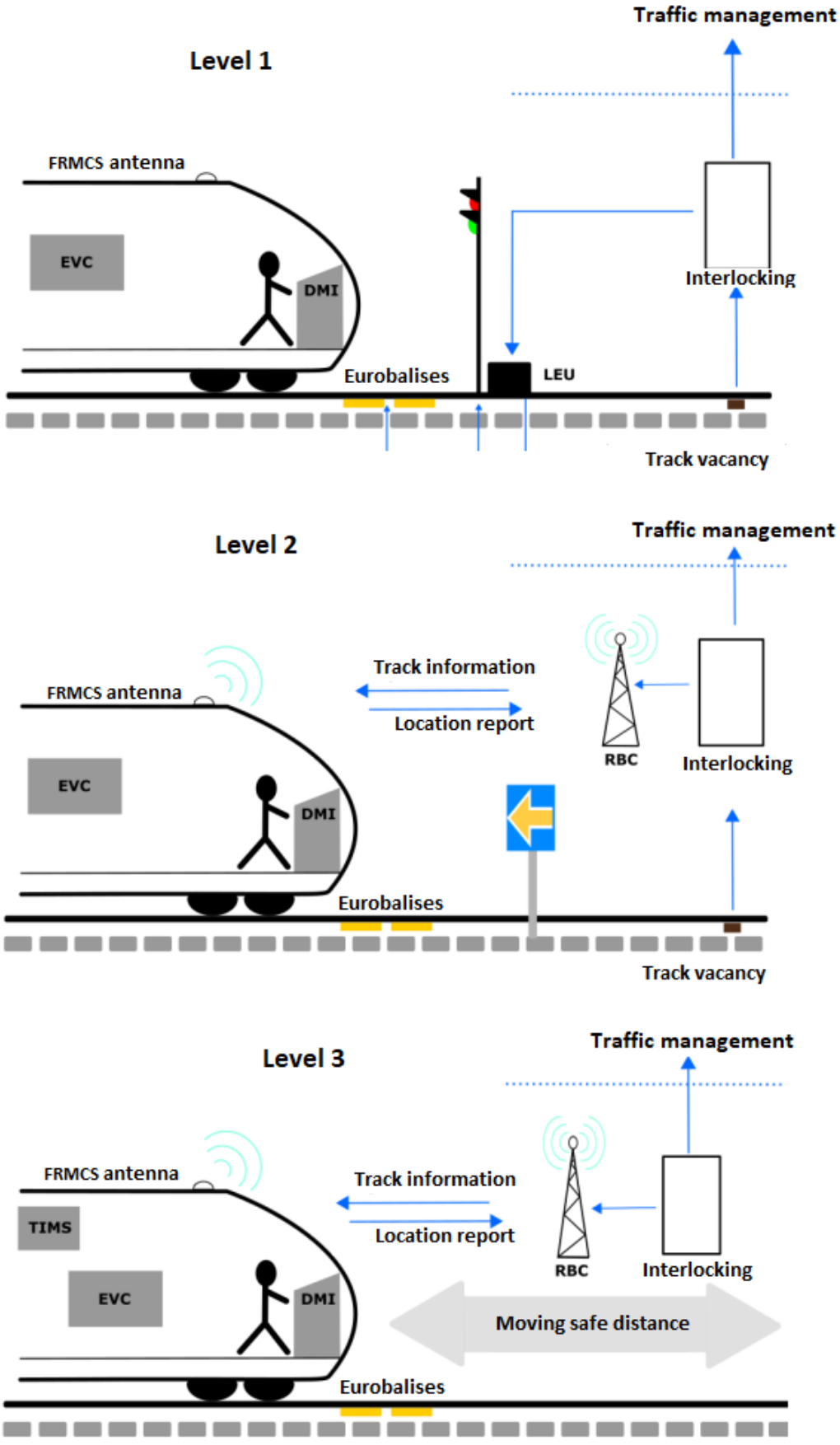

Figure 1. ETCS levels [1]

ERTMS/ETCS level 1 is the most basic one. The communication is done between interlocking through the lineside electronic unit (LEU) to the eurobalise to the train driver machine interface (DMI). The European Vital Computer (EVC) is the central computing unit on the train. The level 1 of ETCS technologies matches the current ATP system used in Finland. The biggest differences between levels 1 and 2 are the technical solutions with the train protection. On level 2 the train and trackside use radio network to communicate.

The communication and the train protection changes from single point centric to a continuous as we move to level 2 and forward. The continuous train protection is enabled by the radio network that is used for communication. As we can see from the figure 1 communication is done from the interlocking through the Radio Block Centre (RBC) and the radio network to the train. One difference between levels 2 and 3 is position data which is supposed to come from the train itself that is used for train control. Another difference is that a Train Integrity Monitoring system (TIMS) is added on level 3.

The above images are a good presentation of the different ETCS levels, but they don’t show the whole ERTMS architecture that well. The risk assessment of ERTMS-based railway systems from a cyber security perspective study was conducted by City, University of London [46] and it has an overall presentation of the ERTMS system Figure 2. The figure shows the different subsystems of the ERTMS architecture.

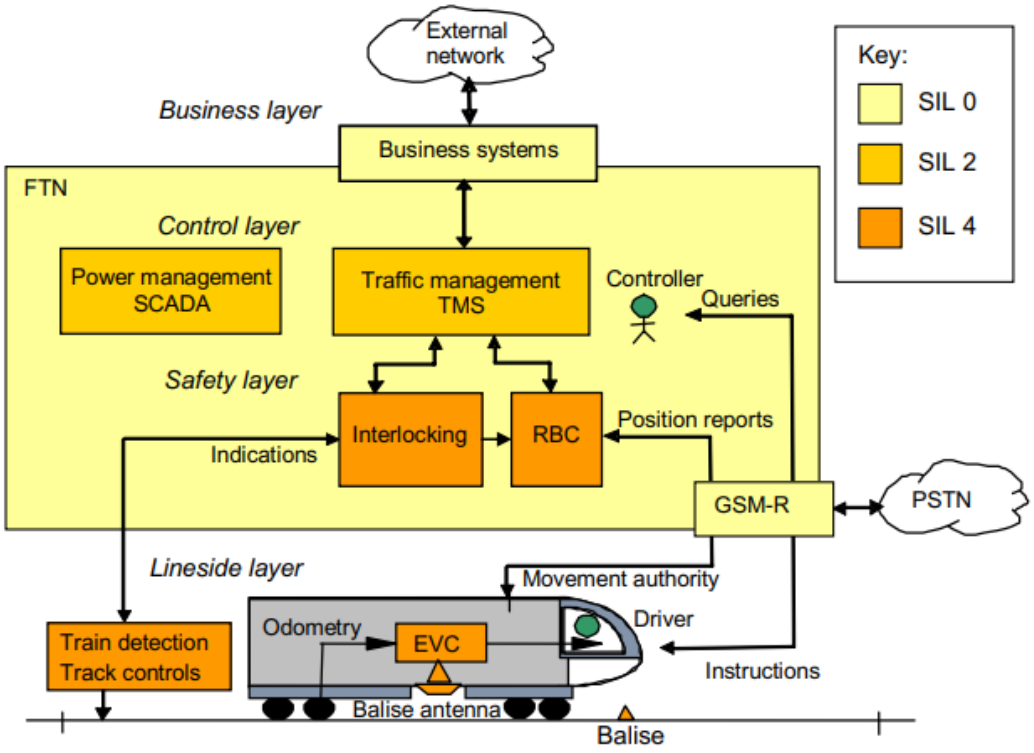

Figure 2. ERMTS-enabled railway signalling system overall architecture [46]

The different SIL levels on the architecture image mean different security integrity levels. The architecture image also illustrates the connections between different parts of the overall architecture. Understanding the connections gives a better view of the cybersecurity of the overall system.

2.2.1 FRMCS

Like mentioned earlier FRMCS will be the new radio communication standard for railways, and it will be also used in Digirail. Global system for mobile communications-railway (GSM-R) is another standard for radio communication in railways and FRMCS is planned to be successor for GSM-R. The goal for FRMCS is to use 5G technology for the communication which means it will support voice and data applications used for railways better than GSM-R. FRMCS is still in planning phase, and it won't be ready for use in few years [36].

2.2.2 Train and trackside connection

According to the document [36] the RBC is a crucial part of the ETCS levels 2 and 3 when the communication between train and trackside is done via radio network. RBC is the part that handles the communication for the trackside equipment and Onboard Unit (OBU) is the counterpart located on the train that communicates with RBC. RBC and

OBU communicate with each other about the location of the train and about the track. The OBU passes the location information of the train to the RBC and RBC gives track information and movement authorities for the OBU.

The communication between RBC and OBU is crucial in terms of cybersecurity since the communication involves the position data and movement authority. Lack of proper security could lead to serious issues. For example, a potential man-in-the-middle (MITM) attack could be performed which means that the data traffic could be hijacked, and the communication altered.

University of Birmingham did research about an attack against message authentication in the ERTMS [49]. In the study they had GSM-R as the communication standard instead of FMRCS. They divided the attack into 4 parts:

- Obtain unencrypted GSM-R traffic
- Observe a collision in the EuroRadio Message Authentication Code (MAC)
- Recover the first of the three triple Data Encryption Standard (3DES) keys, k1
- Forge a Movement Authority message and send it

The study shows that it is possible to observe collision in the EuroRadio MAC and recover the keys of the 3DES. This study applies to FMRCS environment as well if the attacker can obtain unencrypted traffic.

The first part that is sort of a presumption in this attack of obtaining unencrypted GSM-R traffic is not a simple and easy task and the other parts are not possible without it. This means the presented attack is not easy to execute as it might seem, and it is unlikely to happen.

This study does however show that cryptography and encryption are important parts of the overall cybersecurity in railways and finding the proper encryption algorithms and ciphers must be done properly. Encryption also requires distributing the encryption keys to different parties and this might become problematic. If done online and automatically distributing keys requires a key management centre (KMC) that is responsible for creating, distributing and destroying the encryption keys.

Potential attacks against the train and trackside connection can be divided into passive and active attacks. These are generally used terms in IT domains. Cybersecurity study on ERTMS made by Lopez and Aguado analysed [22] different types of attack on the train to trackside connection. Table 1 has a summary of the attacks and their occurrences, impacts and risk levels. As we can see they are divided into passive and active attacks. Passive attacks don’t require interaction with the target, and they are usually

very hard to detect. Active attacks are the opposite, and they directly interact with the target.

Table 1. Summary of train-to-track attacks [22]

Attack type	Means	Occurrence likelihood	Impact	Risk level
Passive	Eavesdropping	Possible	Low	Minor
Active	**Jamming**	Likely	Medium: Force degraded mode	**Critical**
	Spoofing	Possible	High: Wrong driving	**Critical**
	Flooding replay attacks	Possible	Medium: Force degraded mode	Major

Enisa also bring up the importance of protection for the RBC in their document [17]:

“there is high need for protection of the radio block centre in respect of its availability and integrity” Enisa continues about RBC protection and lists the following reasons why it is needed.

If it fails, and especially if it fails on lines without conventional signalling, it would:

- make the line nearly inoperable; trains would have to be re-directed, which would overload other lines;
- mean that the trains on the line in question would have to clear the relevant section, i.e. measures that would reduce the operational safety would inevitably have to be taken.

Cyberthreats must be taken seriously and dealt with properly since there are potentially people’s lives that are in danger in case of an attack. Cyberattack against railways could also lead to financial losses since trains might, for example, get delayed or cancelled and the transportation must be able to adapt for these changes. The communication between RBC and OBU is a crucial part of this.

2.2.3 Traffic control and interlocking

Traffic control is a crucial part of train traffic, and it will improve the capacity by a large margin in the future. According to the finnish document about Digirail [36] the traffic control could increase the relative railway capacity more than the digitalization of railways. It also effects the safety of railways and thus also cybersecurity.

Interlocking is an important part of railway architecture and it does communicate with the RBC and traffic control as can be seen from the Figure 1. Interlocking connects the RBC with the traffic controls and transmits their messages to each other. Interlocking, for example, transmits the information about confirmed routes to the RBC and a potential evil adversary could be able to intervene and cause trouble.

2.2.4 Automatic train operation

Automatic Train Operation (ATO) is another important part of the Digirail project specially from the cybersecurity perspective. Essentially ATO looks to make train operation more automatic and the ATO has different grades based on how much automation and independence it has. The Table 2 is translated from the finnish document about Digirail [36].

Table 2. GoA automation grades [36]

Grade of Automation	Train Operation	Start of movement	End of movement	Door control	Operation during failure
GoA 1	ATP and driver	Driver	Driver	Driver	Driver
GoA 2	ATP and ATO with driver	Automation	Automation	Driver	Driver
GoA 3	Without driver	Automation	Automation	Train staff	Train staff
GoA 4	Without train staff	Automation	Automation	Automation	Automation

During the development and verification phase of the Digirail project, the goal is to reach the grade 2 [36]. With more automation cybersecurity becomes more and more important. On the higher grades when there is less and less staff on the train it becomes very important that system is well protected and access to it is controlled. Specially on the grade 4 when even the operation during a failure situation is handled by automation. This causes threats and a potential evil adversary could take advantage of any potential vulnerabilities.

When a train is driving autonomously it will also require remote monitoring. This is relevant for IT/OT converge context since a lot of the ATO components must be connected and monitored. Cybersecurity practises like access control and authentication become very relevant.

2.3 Cybersecurity in railways

Cybersecurity in general is a quite new topic in the railway industry, and it is something that must be considered when developing future digitalized railway systems. Digitalising railways requires planning and developing cybersecurity solutions along it. Cybersecurity is best when it is planned right from the start instead of trying to add it afterwards. Railway industry has not yet been a huge target for cyberattacks and there have not been that many attacks yet. Here are some examples of the attacks that have happened so far.

BBC reported that in 2015 Ukrainian government was targeted by Denial-of-Service (DoS) attack and railway infrastructure was also targeted [51]. The aim was properly to paralyse some of the critical infrastructure. The attack was larger and coordinated attack by an advanced persistent threat (APT).

SKY news reported that United Kingdom railway network was a target of four cyberattacks between July 2015 and July 2016 [48]. They were thought to be a part of a reconnaissance operation before an actual attack by an APT. The news article about the attack states: “experts have warned that the digital systems controlling trains are vulnerable to hackers, who could cause injury or death in the real world”.

In 2017 Germany’s Deutsche Bahn was targeted by an cyberattack [37]. The attack affected the digital display board. The attacker used ransomware called WannaCry and demanded bitcoins as ransom. The attack claimed that they had encrypted all sorts of files and that they are no longer accessible.

Sweden Transport administration was a target of Distributed Dos attacks (DDos) in 2017 [7]. The first attack had an effect on the IT systems that are used to manage the train orders which caused some delays. The attack also took down Sweden transport administration website and email system thus preventing passengers from making reservations.

In 2018 a DDoS attack targeted a Danish train operating company [12]. The attack prevented the customers from using the ticket machines, website, online applications and some kiosks to buy tickets from them.

In 2020 in the United Kingdom a data breach happened [53]. About 10 000 email addresses and travel details were exposed from people who used the fee Wi-Fi from the railway stations. The breach was possible due to an exposed database and according to the BBC article the database was not protected with a password.

One of the most recent cyberattacks against railways industry happened on July 2021. It was reported by The Guardian [13]. The attack was against the Iran’s transport ministry

and railways. First the attack affected the computer systems of Iran's transport and urbanisation ministry as their website went down. Few days after fake messages appeared on display boards on train stations about alleged delays.

Enisa lists some example cyber risk scenarios in their railway cybersecurity document [42]

- Scenario 1: Compromising a signalling system or automatic train control system, leading to a train accident
- Scenario 2: Sabotage of the traffic supervising systems, leading to train traffic stop
- Scenario 3: Ransomware attack, leading to a disruption of activity
- Scenario 4: Theft of clients' personal data from the booking management system
- Scenario 5: Leak of sensitive data due to unsecure, exposed database
- Scenario 6: Distributed Denial of Service attack, blocking travellers from buying tickets
- Scenario 7: Disastrous event destroying the datacentre facility, leading to disruption of IT services

These scenarios are similar to the listed example attacks earlier. For example with the likes of DDoS attacks and ransomwares which are quite common nowadays in general and not just in railways. The attacks target different parts of the overall railway environment. Some of them target the ATP systems like ETCS and some of them are against the customer's ticket buying systems. This shows that railway is a big overall system that has lot of different subsystems, and this increases that attack surface.

The example scenarios, however, highlight the potential danger for cyberattacks. In the end in none of the real attacks listed earlier caused any real physical harm. Looking at the first example scenario by Enisa [42], however, says that compromising a signalling system causes a train accident. This is a very real threat and must be taken into consideration. When railways become more digitalized more cyberthreats become relevant and attacks against railways will become more frequent as the attack surface becomes bigger.

2.4 IT and OT convergence

OT devices and systems have been isolated for a long time and they might have been designed many years ago. Therefore, there are not many people with proper understanding of them. The access to these systems has been restricted to small number of people. However, these things are changing since OT is becoming more connected with IT. The change has also been called the fourth industrial revolution or “industry 4.0” [32].

IT and OT systems are different in the way that IT is focused on information and OT focuses on the hardware and software that are used for controlling physical equipment. IT and OT converge is a difficult challenging task and it causes a lot of cybersecurity challenges. IT and OT are not just different systems but have different people involved with them. IT team and OT team might be completely separated and have nothing to do with each other. Merging the people behind the systems is an important part on converging the systems. IT workers must be aware of OT and wise versa. IT and OT have been getting more overlapped in many industries recently and will surely keep doing so. Bogen highlights that even though IT and OT have been getting more overlapped, there are still different aspects that must be considered, and the IT cybersecurity cannot just be slotted on [6].

Converging IT and OT must be done properly since they are different kinds of systems from the perspective of cybersecurity. We can see in Figure 3 an example by Otorio [33] listed on their website about IT and OT systems and how do they overlap. We can see that the typical IT systems are more focused on software side whereas OT is more oriented with the physical world.

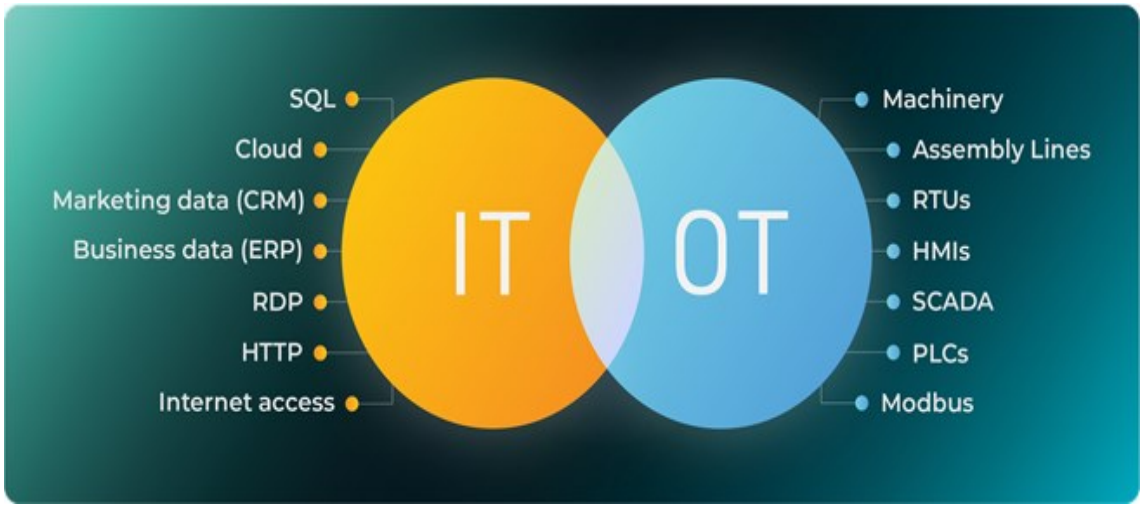

Figure 3. IT and OT converge [33]

Converging IT and OT is not just a challenge however, but it also comes with benefits. International society of automation ISA has a post on their website about IT/OT converge [45] and they list the following benefits that come with converging IT and OT systems:

- Streamlined processes, resulting in greater efficiencies
- Lower fixed costs through elimination of redundant systems
- Ease of performing security and other analytics
- Facilitation of business process engineering through advanced use of analytics in OT systems
- Transfer of best practices to OT (e.g., patch management)
- Real-time tracking of OT devices

This list is a more general one and not a specific for railway environment or Digirail but gives a general overview of the situation. We can see that connectivity is not just a risk but also an opportunity. Being able to remotely monitor and control devices eases the processes. But even with the benefits the connection must be done securely. The same article [45] also has a list of the risks that come when the merging of IT and OT is not done properly:

- Disruption of Industrial Control Systems ICS due to blocked or delayed flow of information through ICS networks
- Unauthorized changes to instructions, alarm thresholds, and logic, with the potential of endangering human life
- Inaccurate information sent to system operators, causing the operators to initiate inappropriate actions, which could have various negative effects
- Unauthorized modification of configuration settings
- Interference with operation of safety systems, among other key functionalities
- Legacy devices that are not designed securely may be used as a platform for launching cyberattacks.

The problem is when merging the two that the converged system might have bad management and bad technique. The challenge is to get the better parts from both worlds. Cyberattacks have been the mostly only targeted against IT systems until recent years.

Nowadays OT systems must be secured properly when connected to IT so that they are not vulnerable for cyberattacks.

STUXNET was the first big cyber-attack against an industrial environment. STUXNET is a malicious computer worn which targets supervisory control and data acquisition (SCADA) systems [16]. It is a virus that could, for example, inject to the system via USB flash drive and it does also spread on its own after it has injected to the system. It was first discovered in 2010 when it was used to infect several different industrial sites in Iran like, for example, an uranium-enrichment plant.

Poneom institute conducted research on energy and utilities, industrial and manufacturing, health and pharmaceutical, and transportation sectors [14]. They found out that 90% of them suffered a damaging cyberattack in the past two years. The industries that participated in the study have a lot of operation with OT so that means attacks against IT would also be dangerous because of the connectivity between IT and OT. They also reported that half of the participants had had a cyberattack against their OT systems that caused downtime.

Half of the participants also said that downtime is highest risk for their operation. This is relevant for railways as well since downtime caused by cyberattacks in railway environment leads to delays and that leads to time and financial losses to the customers as well to the railway operators. It is quite concerning how big effects cyberattacks can have against industrial and OT systems.

The research [14] also stated that the organisations found attack against OT assets as one of the most worrisome threats for them. This goes along with the statement that attacks against OT have generally higher ceiling for how destructive they can be.

Coy and Gadbois have an article about Connectivity & Cybersecurity and IT-OT Convergence [8]. Figure 4 is from the article and it is an example of what architecture could be like when OT and IT are converged, and it shows the different barriers between the networks. The different zones can be seen from the image that are typical for these kinds of industrial systems. Firewalls are one example of these barriers, and they can be seen in the figure for separating the sites A and B from the trusted IT network. Firewall does not guarantee 100% security, but it will surely make the system safer.

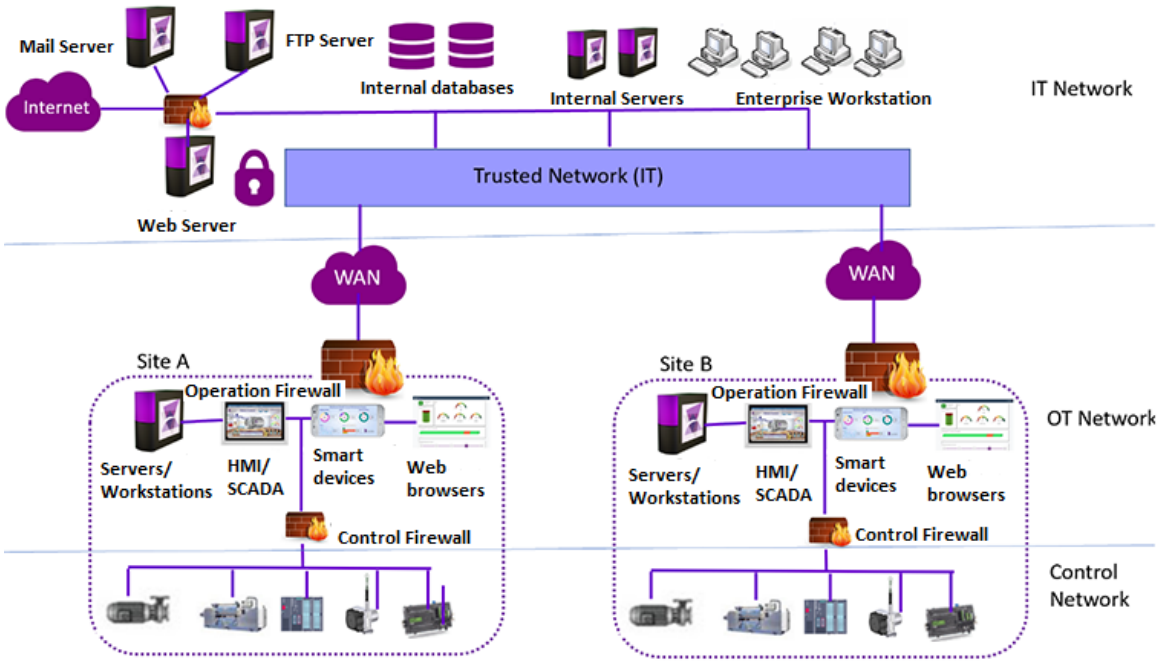

Figure 4. Example OT/IT converge architecture [8]

2.5 IT security vs OT security

IT security and OT security have several differences and the effect of a possible attack is a significant one. Attack against IT might lead to some data stolen whereas attack against OT systems in a worst case could lead to a breakdown of an industrial system like nuclear system thus causing serious physical harm. Even though IT incidents are more frequent, OT incidents can be a lot more destructive. OT systems don't only operate in the digital world but also in physical world. It is important to understand that unlike IT systems OT can have impacts on physical world as mentioned earlier in this thesis.

The cybersecurity issues in IT and OT are not that different from each other and they overlap. It is said that 80% of the cybersecurity issues faced by OT are identical to IT [20]. It might not by exact number, but it gives an idea and it does make sense since the OT has been adapting IT technologies.

Whitelisting vs blacklisting is one principle that separates IT and OT from each other. Whitelisting goes with the principle of deny by default which means that an asset needs to have certain permission to be used. This is useful for OT environments since they are more static. Blacklisting on the other hand means, for example, that only known malwares are blocked and other software is allowed by default. Blacklisting is used in IT environment since there are other practises for scanning and finding new vulnerabilities.

Otorio [33] website also lists some core differences between IT and OT systems. When talking about cybersecurity of IT systems the main point is to prioritize confidentiality and

on OT systems the focus is on safety. Attacks against IT systems might not really cause any physical harm, but confidentiality and availability of data can be at risk. Attacks against OT on the other hand can cause more physical harm. OT cyber incidents in general have higher ceiling for how destructive they can be. That is why converging OT with IT is a challenge.

OT is usually more vulnerable because cybersecurity has not been designed into them. Because they have been isolated from the internet and not connected with IT, vulnerabilities are not directly exploitable. Cybersecurity is important for both types of systems, and a cohesive solution where both sides are considered is a challenging task, but it can be overcome. [6].

Another difference between IT and OT is the lifecycle. IT devices are usually replaced every few years whereas OT devices can run for decades even without being replaced. This connects closely to patching which is another thing that is completely different in the two worlds. Most IT systems have regular patching schedules and OT on other hand have very rare patches and might have none at all. Lack of proper patching also leads to more vulnerabilities which is something that needs to be addressed when connecting OT with IT.

The Dutch security cluster called Security Delta (HSD) released a report on OT and IT integration and its implication for cybersecurity in 2021 [2]. In their report they talked about the differences of OT and IT security. Table 3 is from the report and it shows a summary of the differences about IT and OT security.

Table 3. OT security VS IT security [2]

	OT	IT
Anti-virus	Often difficult or impossible to use in (legacy) systems	Is used everywhere
Vulnerability scanning	Passive scan as an advice, an active scan could disrupt the operational production	Active scan
Network an asset scanning	Passive scan	Active scan
Patching	Slowly, or not possible (anymore), and requires supplier approval	Frequently, even daily
Reliability	Failure is unacceptable	Incidental failure is accepted
Availability	24 / 7 / 365	Planned downtime is OK
Security testing	Only after very careful considerations and after identifying risks	Is widely used
Performance	Large delay is a serious problem	Large delay and instability are acceptable
Security	Information system network is isolated from plant network	Little separation between networks at the same location
Security and awareness	Bad	Reasonable to good

From the Table 3 we can see that OT systems, for example, have to be available basically always whereas IT can have planned downtimes and how failures are not acceptable for OT. It might not be as strict as it says but it is true that uptime is very important for OT as mentioned earlier. The table illustrates well how vulnerable and fragile OT systems really are. The isolation has really been the main protection method for OT system a long time and will probably be in the future since it might not be possible to remove. These topics shown in the table are topics that must be assessed and planned when planning an OT/IT converge. This table represents a typical environment but there are of course exceptions where all of these don't apply.

2.6 IT and OT systems in Digirail environment

IT systems in Digirail are the systems that support the operative systems and connect the operative systems. OT systems are the operative systems that control the traffic infrastructure and moving equipment. Traficom lists some example systems of IT and OT in their document about promoting of cybersecurity recommendations [47]. Some examples of the IT systems are passenger information, drivers end device applications, general communication methods like Wireless Local Area Networks (WLANs) and information and communication systems. OT system examples are ERTMS, ATP, remote control and interlocking

Digitalization is starting to affect the railway industry and railway systems are becoming more digitalized and connected. IT and OT systems in railways are converging and that influences cybersecurity. IT and OT converge in a transportation industry such as railways must be securely and properly. Leaving railway OT systems vulnerable could cause serious harm since attacks and incidents for OT systems are more severe than for IT systems. Attacks against railway systems could cause severe physical harm like, for example, a train accident [42].

Asset management becomes very relevant with IT/OT converged railway systems. The ability to manage all different assets in a railway is crucial for security. ABB and Microsoft released a survey report on IT-OT converge on railways [31]. The results showed that the importance of asset management is growing a lot and the value of IT-OT integration is big for asset management.

As mentioned earlier, connecting IT and OT systems has benefits too and there are reasons why it is happening. Being able to transfer data between IT and OT means better monitoring and collecting data from the railway equipment. It also supports the further automation and digitalization of the rail industry in the future. The IT and OT systems

overlap in railways when, for example, a control system is connected to a network or when a sensor sends data to the cloud. The overlap or the interface between the two systems must be managed properly since it must respect both worlds and their overall cybersecurity requirements.

Figure 5 has examples of both IT and OT systems that are relevant for railway environments. A single part of the overall railway system can be on the overlapping area of IT and OT and that is why finding the best practises from both areas is important so that cybersecurity can be managed coherently.

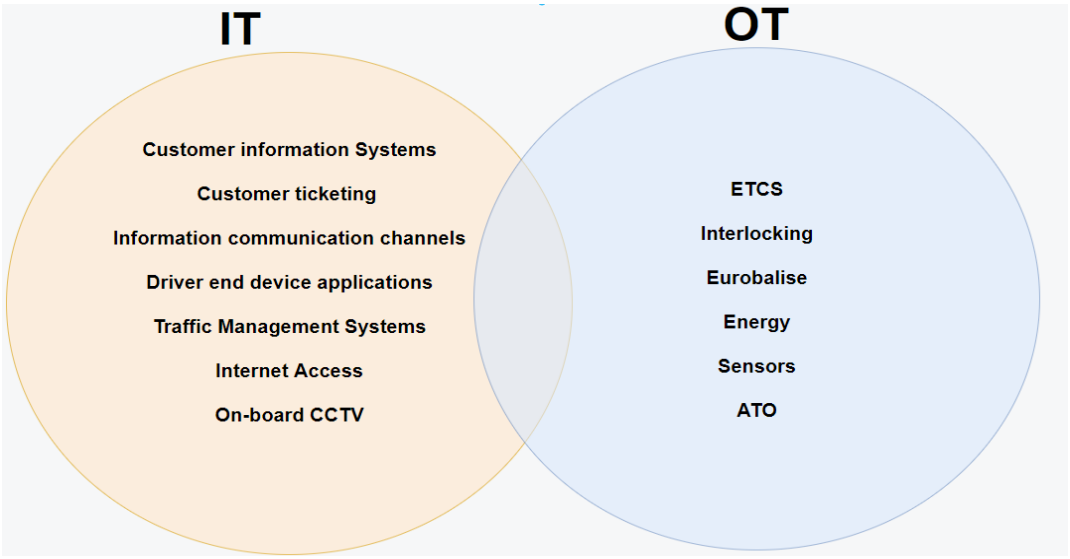

Figure 5. IT and OT systems in railways

3. RESEARCH

This research focuses on the best practises of IT and OT systems' cybersecurity for Digirail. The main guideline for this research is the railway specific cybersecurity standard TS50701. The TS50701 standard is assessed to see how well it includes the cybersecurity practises from IT and OT sides. Other standards that are used as additional source of information are IT cybersecurity standard ISO/IEC 27001 and OT cybersecurity standard IEC 62443. Other guidance and articles that can be found on the topic are used as an additional source of information.

Another way of collecting data for this research was interviews. In this research interviews are used to collect data from different specialists working with Digirail about the OT/IT converged Digirail environment and the challenges and practises involved. Since cybersecurity is a new topic for railway and the OT/IT converge and overlap is a big factor for this it is important to understand overall system better. Therefore, interviewing the different professionals about the challenges and ways of converging OT and IT is important.

3.1 Other research on the topic

There has not been much of this kind of research since the focus of this thesis is on the new cybersecurity standards and the overall scope of this thesis is quite new. One similar research was found called "Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: Cybersecurity Best Practices and Risk Management" [21]. It had similar scope to this thesis, but the focus was on marine energy instead of railways.

As a result, from the research there were several different cybersecurity practises found like, for example, asset management, access management and incident management. These are all topics that are relevant in the railway environment as well.

3.2 Interviews as a research method

There are different types of interview methods such as structured interviews, semi-structured interviews, and unstructured interviews. They all have their different advantages and disadvantages. Structured interviews have prepared questions, and the structure is fixed. This, however, limits the type of results from the interview. Unstructured interviews are the opposite where there are no guidelines or questions prepared beforehand. This

may help with getting more detailed answers, but it might be harder to focus on the topic [10].

The semi structured interview method combines the prepared questions with the openness, and it encourages a two-way conversation. Kakilla mentions [9] that semi-structured interviews are good for in-depth conversation. The goal for the interviews in this study is to have more of a conversation about the topic than just ask questions. These are the reasons semi-structured interview was chosen as the interview type for this research.

4. TS50701 STANDARD

This chapter focuses on the overall studying of the new railway cybersecurity standard TS50701. It is important to study the standard since it is the most relevant part and the main focus point for the outcome of this thesis.

This chapter handles the standard for its most relevant and most interesting parts. The focus of this thesis which is the IT and OT cybersecurity practises is kept in mind and all the topic relevant for that are covered. The chapter starts with the overview and introduction of the standard and then goes through the different parts of the standard. This chapter gives a good quick summary of the contents of the TS50701 standard.

4.1 Overview of the standard

Since cybersecurity is becoming more and more relevant in the railway sector a proper standardization for railway cybersecurity is needed. That is why the new TS50701 is an important step for railway cybersecurity since it has requirements and recommendations for cybersecurity in railways. The TS50701 standard is provided by the European Committee for Electrotechnical standardization (CENELEC).

TS50701 [11] includes guidance on how cybersecurity should be managed with the context of EN50126-1 Reliability, Availability, Maintainability, Safety (RAMS) lifecycle process. TS50701 standard takes inspiration from the standard IEC 62443 standard series and adapts the contents to railway industry. The security management requirements of the TS50701 standard are based on IEC 62443-2-1 which is further based on ISO/IEC 27001.

The TS50701 document [11] includes a table that is an overview of descriptions, synchronization points and deliverables for cybersecurity actions in railways. The framework of the table is based on EN 50126-1. The table is kind of an overview of cybersecurity activity lifecycle in a railway system.

TS50701 standard includes guidance for security-related applications conditions (SecRACs). They can be either technical countermeasures introduced outside of the system under consideration (SuC) or organisational and procedural countermeasures like IEC 62443-2-1 and IEC 62443-2-4. A combination of these is also a valid solution.

4.2 Network segmentation and DMZ

Network segmentation is a part of the best practises for cybersecurity, and it is covered in the TS50701 standard. TS50701 [11] shows a proposed segregation for IT and OT systems in the railway environment. It shows that ISO/IEC 27001 could be used as a guidance for the IT side and TS50701 and IEC 62443 as guidance for OT side. IT and OT are also connected in the presented architecture in TS50701.

An IT/OT industry expert Mike Smith wrote an article about best practises for IT/OT converge [41]. He talks about assessments of the network and segmenting the network. He also brings up another interesting topic for IT/OT networks which is a Demilitarized Zone (DMZ). DMZ in computer security means a logical or a physical zone that is used to separate the local area network from untrusted traffic. DMZ is sort of like a buffer between the internet and private network [4].

Separating the OT and IT environments with a DMZ could make controlling and monitoring the traffic easier and thus reducing risks for any potential cybersecurity incidents. DMZ is often between two firewalls like shown in the Figure 6.

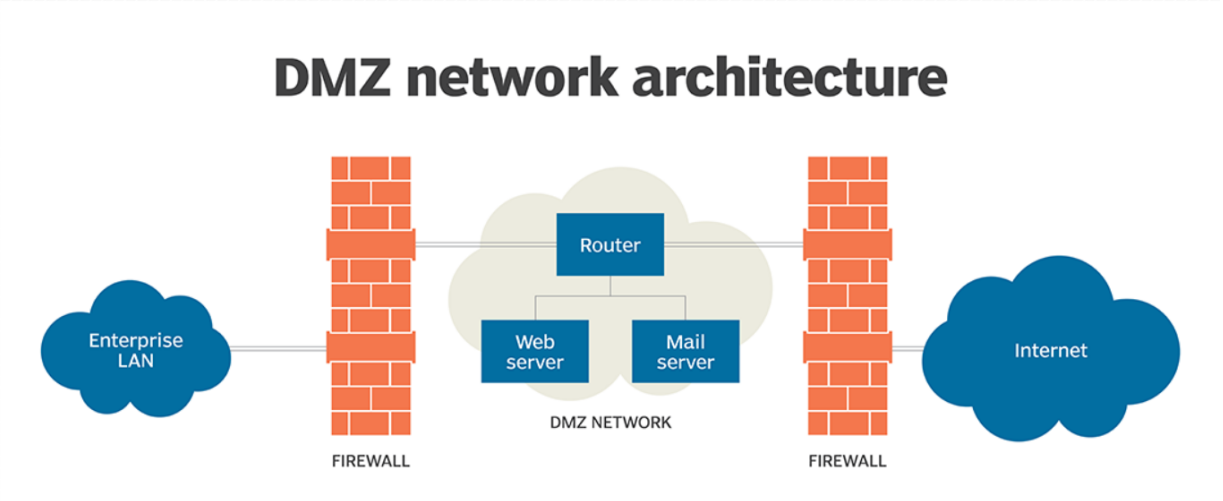

Figure 6. DMZ architecture [4]

Network segmentation and DMZ are topics that are important for railways since it is a critical environment. It is mentioned as a good cybersecurity practise or as a solution in several different sources and articles like in Shift2Rail document [15].

Mattei mentions network segmentation as one of the cybersecurity solutions [40]. Another topic that Mattei brings up is the importance of planning the connections properly.

Creating new connections should not be done carelessly but instead should be planned and done according to a framework.

4.3 Asset management

Asset management is an important part of cybersecurity. Asset management is a quite broad concept and is not limited to just IT or OT environments. Asset management is about policies and processes behind the system. Protecting a system with proper asset management is a lot easier than one with no asset management. When searching for good cybersecurity practises, asset management often comes up. For example, Mattei mentions [40] how understanding all assets in the system is good strategy for cybersecurity.

Asset management is important for railways as well and it is covered on the TS50701 standard. The Figure 7 is based on the TS50701 standard [11], and it models the different assets of the railway environment. The different assets are divided into different colours based on their function that are signalling, command and control, auxiliary, comfort and public. The meaning of different colours can also be seen from the white box at the bottom left corner.

They are also grouped into different zones that represent the assets' physical location on the overall system. We can see that there a lot of different assets in the railway environment and that only makes the cybersecurity more important.

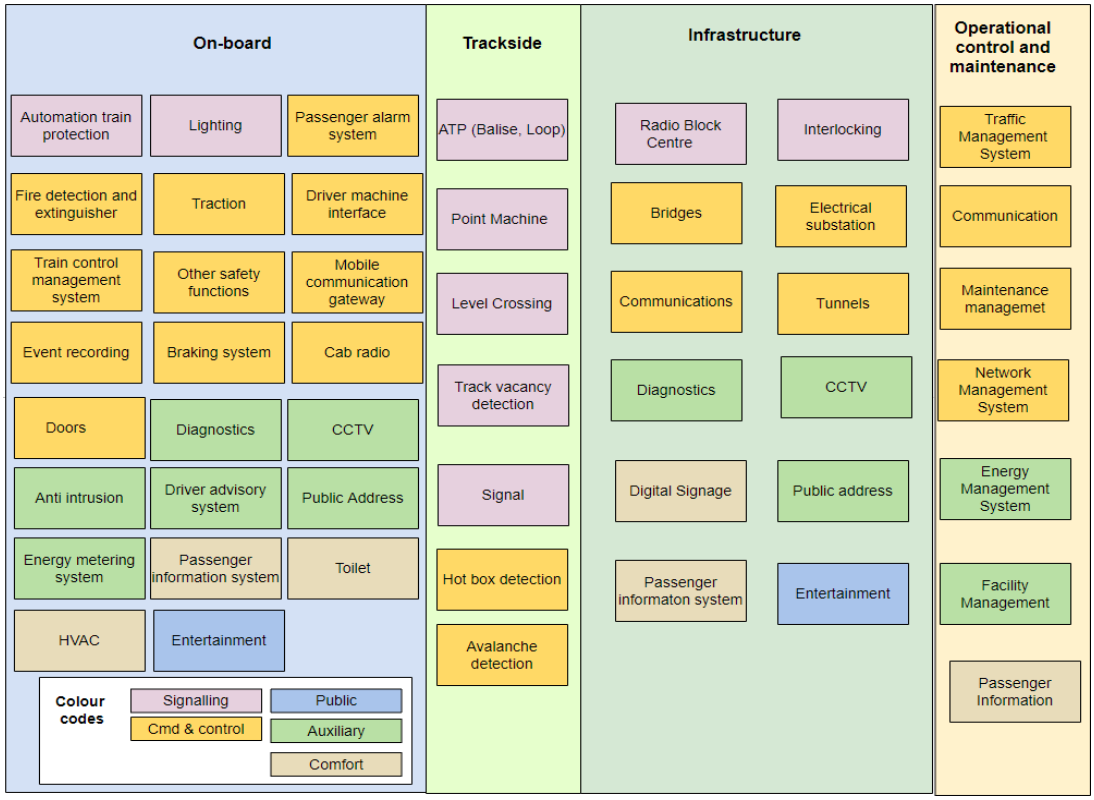

Figure 7. Railway asset model [11]

The asset model example however doesn't have all the relevant assets in it. Key management system, antivirus and data management are some examples of the assets that are relevant for railway cybersecurity and are missing from the model. The TS50701 standard is a new standard, and it will continue to be developed so the missing assets are probably going to be added in the future with new versions of the standard.

4.4 Risk assessment

The high level risk assessment process does not really change depended on whether the system under consideration is IT or OT related or both. The TS50701 standard provides steps for an initial risk assessment. The Figure 8 that is from the TS50701 standard [11] shows the initial process of risk assessment. The process is corresponding to the IEC 62443-3-2 and the zone and conduit requirements (ZCR) are defined there. The standard covers the process more in detail.

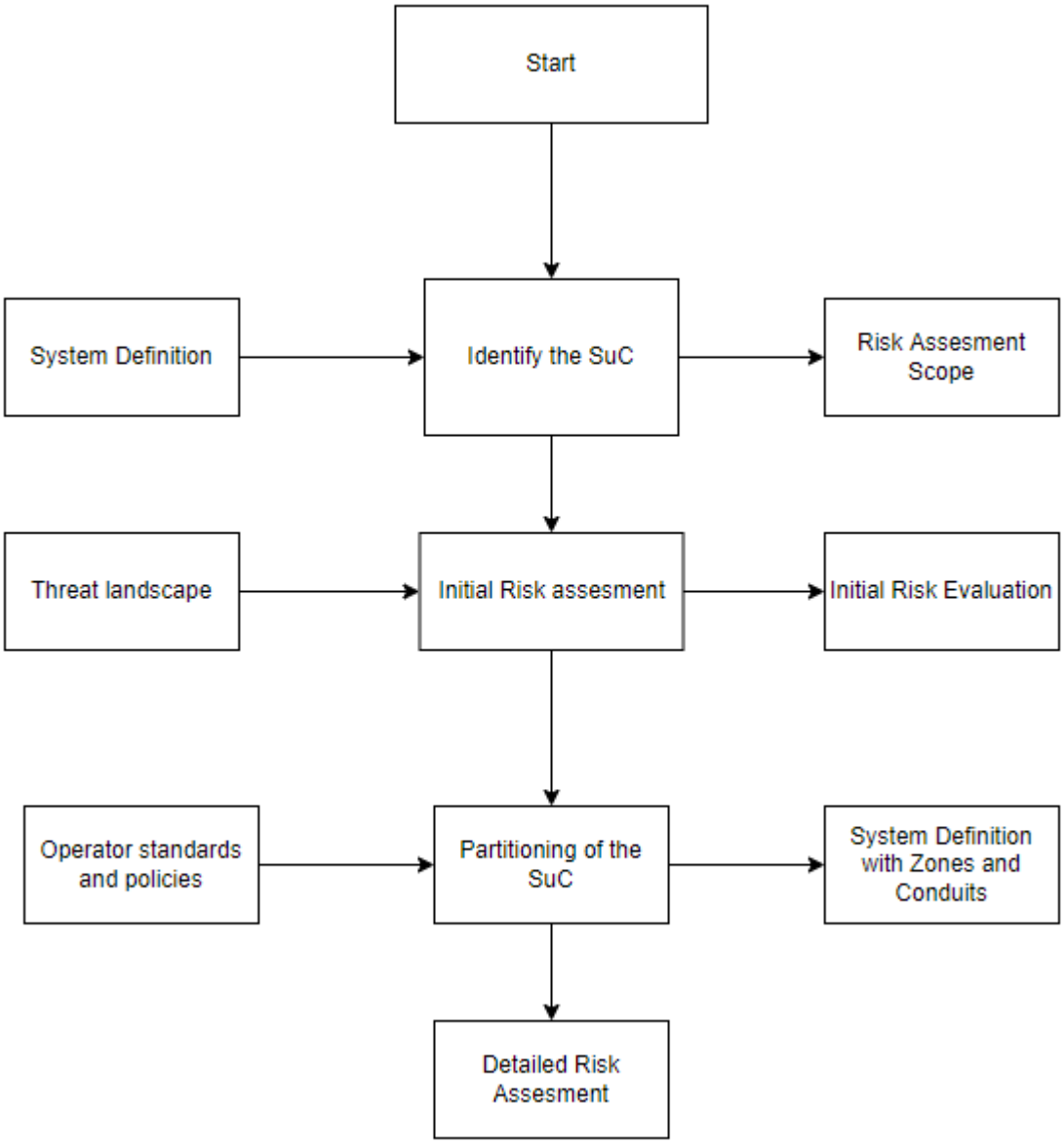

Figure 8. Initial risk assessment [11]

TS50701 standard also provides good impact and likelihood assessments. Overall risk management is done quite deeply in the TS50701 standard [11]. Most of the risk assessment topics are referred from the IEC 62443 standard so the railway industry is not so different from a typical OT system from the perspective of high level risk assessment for cybersecurity.

The standard has own whole chapter for detailed risk assessment which is the most bottom part of the process chart of the risk assessment. The detailed risk assessment has an own flowchart in the TS50701 standard document [11]. The detailed risk assessment involves topics such as threat identification. Overall, the risk assessment in covered very in depth in the TS50701 standard and it has been divided into several parts different

processes. Since risk assessment is not strictly just IT or OT related TS50701 covers the well for railway needs.

4.5 Access control and authentication

Access control is an important part of cybersecurity, and it is important for both IT and OT even though it traditionally can be thought more as an IT side of cybersecurity practise which involves, for example, passwords and user credentials. There are different types of access control. For example, fourwallssecurity [38] lists the following types.

- mandatory access control: In this method of access control there is a central authority that control the access based on different security levels.
- role-based access control means that the access is granted based on the position and role of the individual. The access is only granted for those that it is necessary for their role.
- discretionary access control means that there is an owner or an administrator that sets the policy of who has access to data.
- Attribute-based access control means that the access is based on dynamic attributes such as environment conditions.

This is only one of the ways to classify access control and there are also several other ways of how to classify and divide the different types of access control.

In the list of system security requirements found on the TS50701 standard [11] there are several requirements related to access control like authentication and human user identification. The annex C of the TS50701 standard which is the cybersecurity design principle annex lists access control as a guideline for railways. The annex C of the TS50701 standard has a smaller part C.8 for access control. One design principle example mentioned is how access can be physical and remote. This shows that access management for railways is important for both the physical and the digital world. Physical access to a railway equipment must be controlled properly or it could be taken advantage of and caused a lot of harm. The TS50701 standard [11] lists about the following practises for implementing access control for railways:

— Authentication and Authorization

— Network access controls

— Physical countermeasures

Authentication is a process related both to IT and OT and the TS50701 standard takes it into account. It has additional railway related requirements for authentication and multifactor authentication. The standard [11] gives several examples of authentication methods for railways in the section C.7. Some examples are ID and passwords for users and digital signatures for more software side. Authentication is related to both IT and OT but the better practises for it come from IT side like, for example, passwords. This is well instructed in the TS50701 standard overall.

Access control overall is well covered in the TS50701 standard, and it has several cybersecurity requirements towards specifically railway systems. There are several references to the IEC 62443 standard and the TS50701 standard lists several requirements and instructions for access control that considers the IT side as well.

4.6 Vulnerability and patch management

It is important to understand the different vulnerabilities that appear in the environment and classify them and the TS50701 standard [11] mentions that proactively handling with vulnerabilities is the goal. Like stated earlier in this thesis the vulnerabilities for IT and OT are similar and they do overlap. Since they are similar and mostly shared, they need a shared vulnerability management for them as well.

Patch management is a critical part of protecting a system against cyber threats. Patch management really shows that cybersecurity is not something that can just be slotted in and then forgotten about. Cybersecurity must be constantly kept up to date and vulnerabilities must be patched. OT systems have had the tendency of not being patched and just left alone thus increasing the vulnerabilities with them. Having a proper patch management greatly enhances security and decreases the number of vulnerabilities in a system.

Patch management is something that has not really been a part of the railway industry until now. Railway digitalization just like every other form of digitalization must take patch management seriously. The TS50701 [11] clause 10 operational, maintenance and disposal requirements have one subclause for vulnerability management and another subclause for patch management. The Figure 9 is from the TS50701 standard [11] and it shows the flowchart for handling vulnerabilities. Managing vulnerabilities is closely connected to managing and assessing risks. Patch management can be thought to function with vulnerability management. The figure has the most bottom part “implementation and monitoring”. This goes with the mindset that cybersecurity is not a plug in and leave principle but instead a constant cycle of monitoring and improving.

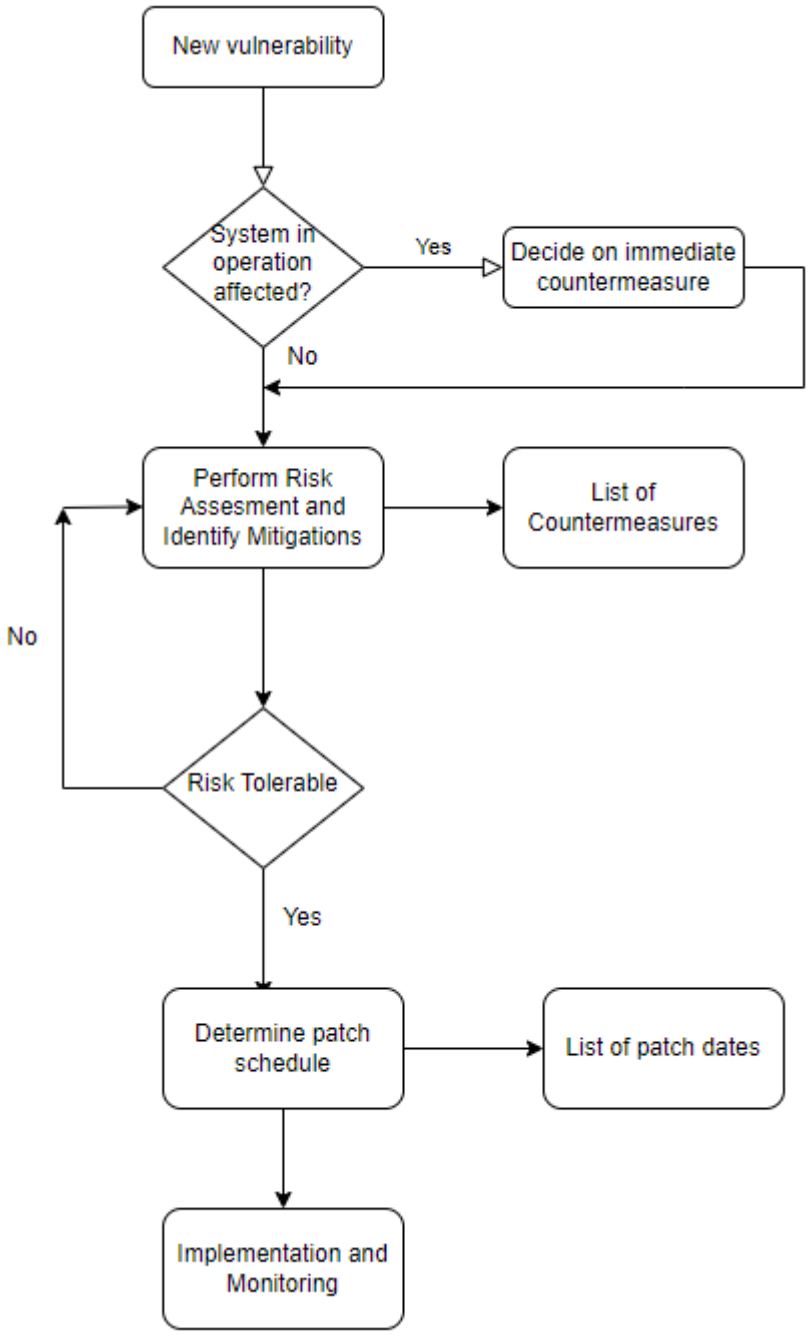

Figure 9. General vulnerability handling flowchart [11]

Like mentioned earlier, when considering OT systems as isolated systems, they are very rarely patched and could have a lot of vulnerabilities because of that. With increasing connectivity between IT and OT this must be changed. Patch management has usually only really been relevant for IT systems but now OT systems are becoming more connected and require better patch management. The biggest difference between IT and

OT patch management has been the frequency of patching. IT patching has certain routines like the “patch Tuesdays” with Microsoft, adobe and oracle systems [5]. Regular and routine patching has been a normal for IT systems for a long time whereas in OT the patch management is almost non-existent.

Availability and uptime for systems are crucial in a railway environment. This ties closely to patch management and it must be taken into consideration. Figure 10 is from the TS50701 standard [11] and it shows the update timeline and the outage period within. The orange arrows show when the system is vulnerable and green when it is secure.

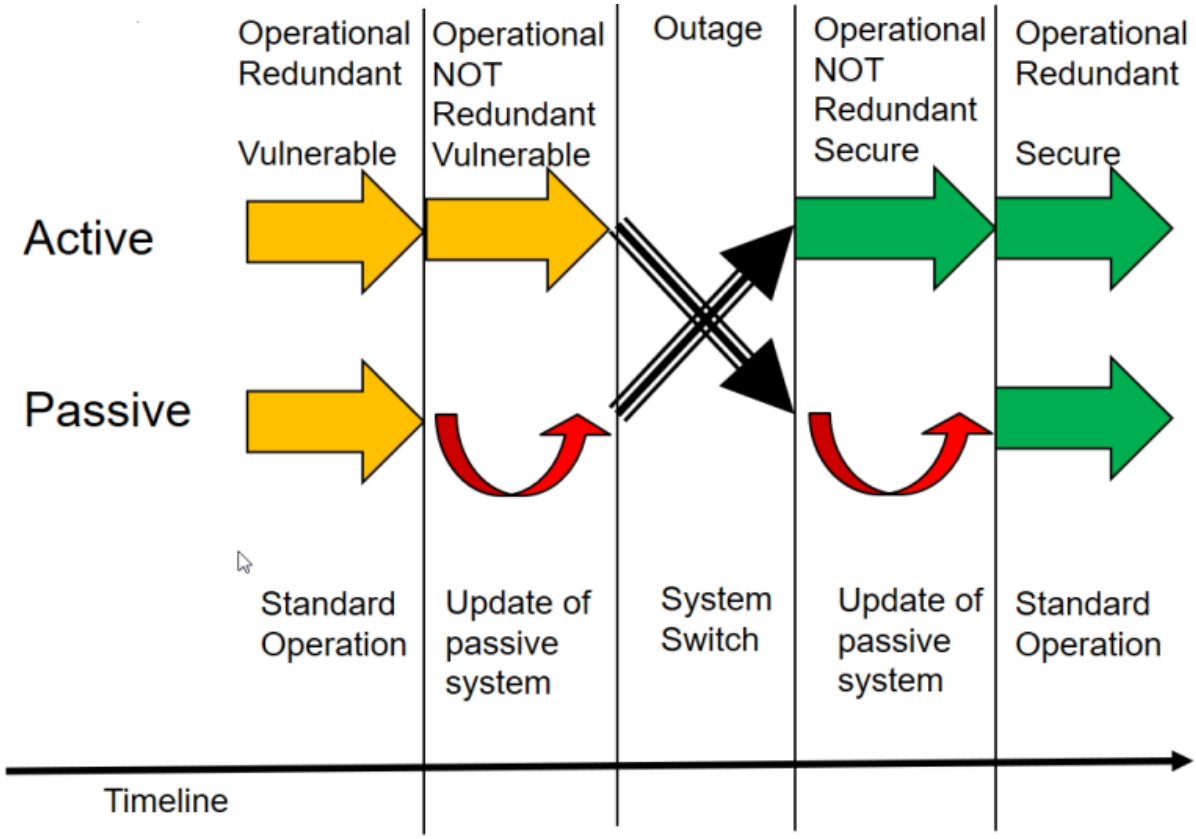

Figure 10.Vulnerability and outage time during system update example [11]

When IT and OT become more connected, they require homogenous patch management. IT systems have generally better and longer experience with patch management and thus better practises for it. OT patching is difficult since the devices might not always be compatible with all the patches, and it might get expensive and difficult to patch OT systems. OT could use alternative answers for patching to reduce the risks if patching becomes too difficult but if a certain device or subsystem of railways overlaps with IT and OT it should be patched according to IT patching practises.

One of the biggest challenges with vulnerability management for railway systems is how to react to a cyberattack or an incident. Reacting to attacks that are solely against IT systems is different than a converged IT/OT railway environment. With IT you can just turn of the PC and disconnect it from internet but with railways you cannot just take a train out the system and throw it away. Therefore, proper risk management beforehand and handling vulnerabilities with patching in advance is crucial. The current version of the TS50701 standard [11] does not have a proper section for incident management and it states that it will be added in later versions.

4.7 Backups and recovery

Losing data or the access to data can have big consequences. Data backups are one of the most widely used methods to enhance the availability and integrity of data. A lot of people use different platforms like clouds, flash drives, or external hard drives for backing up their data. However, backups are not just meant for data but systems as well.

System backups are meant to restore the integrity of a system in case a hardware or software failure, physical failure or a human error occurs. Specially for OT systems the system backups and that they are up to date is essential. The different subsystems in railway environments need proper backup procedures in case they go down due to a malfunction or even a cyberattack. Like mentioned earlier in this thesis uptime in general is important for OT systems and downtime can have serious impacts.

Data and system backups are important for railway environment and the TS50701 [11] document's security requirements table has four requirements for backups and recovery.

4.8 Cryptography and encryption

Cryptography and encryption can make a big difference to the security of a system. Poor cryptography methods lead to vulnerabilities that can be easily exploited by attackers. The TS50701 standard [11] has System Requirement (SR) 4.3 called use of cryptography which also has additional info for railway systems about cryptographic key establishment and management.

It also brings up advanced encryption standards (AES) which is known to be safe algorithm against brute force attacks and has never been cracked by them [39].

5. ISO/IEC 27001 AND IEC 62443 STANDARDS

This chapter is much like the previous one but this time the focus is on the ISO/EC 27001 and IEC 62443 standards. This chapter goes through the two standards and gives an overview of the standards and a summary of their contents.

Much like the previous chapter about TS50701 the focus is on the IT and OT cybersecurity since it is the focus point of this thesis. The chapter starts with overviews of the standards and then goes through the context to find the most relevant parts according to the scope of this thesis.

5.1 ISO/IEC 27001 standard overview

ISO/IEC 27001 is a well-known information security standard that provides requirements for information security management system ISMS [29]. ISO/IEC 27001 is a part of the ISO/IEC 27000 standard series, and it is made by the joint committee of International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC). The ISO/IEC 27000 standard series has several standards, but in this thesis the focus is on the ISO/IEC 27001 standard.

ISO/IEC 27001 is focused on IT systems' security, and it is widely used information security standard on different organisations that need to improve their information security. The standard involves different kinds of policies and processes for organisations to use. The basic goal is to protect the three aspects of information security according to the CIA model [18] which are confidentiality, integrity and availability.

- Confidentiality means that the secret information is protected against unauthorized access. For example, several access control methods like multifactor authentication protect confidentiality.
- Integrity means that the information has not been changed or modified by an unauthorized party. Encryption is an example for this. Even if data has been leaked, a strong encryption saves the integrity of the data because it cannot be modified.
- Availability is that the data, systems, and applications are available to the users when they need them. A DoS attack is a good example against the availability and planning and preparation against such attack is a way to protect the availability.

ISO 27001 has 10 short clauses that are the following [30]:

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment
7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

The standard also has controls spread across different groups and categories. In total the standard contains 114 controls in 14 groups and 35 control categories. They are listed in the annex A of the ISO/IEC 27001 standard [30].

A.5: Information security policies (2 controls)

A.6: Organization of information security (7 controls)

A.7: Human resource security - 6 controls that are applied before, during, or after employment

A.8: Asset management (10 controls)

A.9: Access control (14 controls)

A.10: Cryptography (2 controls)

A.11: Physical and environmental security (15 controls)

A.12: Operations security (14 controls)

A.13: Communications security (7 controls)

A.14: System acquisition, development and maintenance (13 controls)

A.15: Supplier relationships (5 controls)

A.16: Information security incident management (7 controls)

A.17: Information security aspects of business continuity management (4 controls)

A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

These controls include the actual practises for how an organisation can manage their information security. They cover a different aspects of information security and they will be studied later in this thesis.

5.2 IEC 62443 standard overview

IEC 62443 is an international series of standards on industrial automation and control systems (IACS) [44]. Whereas the ISO/IEC 27001 standard is for guidance for IT systems information and cybersecurity the IEC 62443 is for industrial automation systems or also called OT systems and their cybersecurity. The two environments are different as covered earlier and it is relevant that there are different standards for them. The IEC 62443 is partly made with references to the 27001 so some of the parts are similar.

IEC 62443 is developed by the ISA99 committee and adopted by the IEC [44]. IEC 62443 standard series consists of several different standards that can be seen from the Figure 11 that is based on the presentation of the standard parts from ISA website [19].

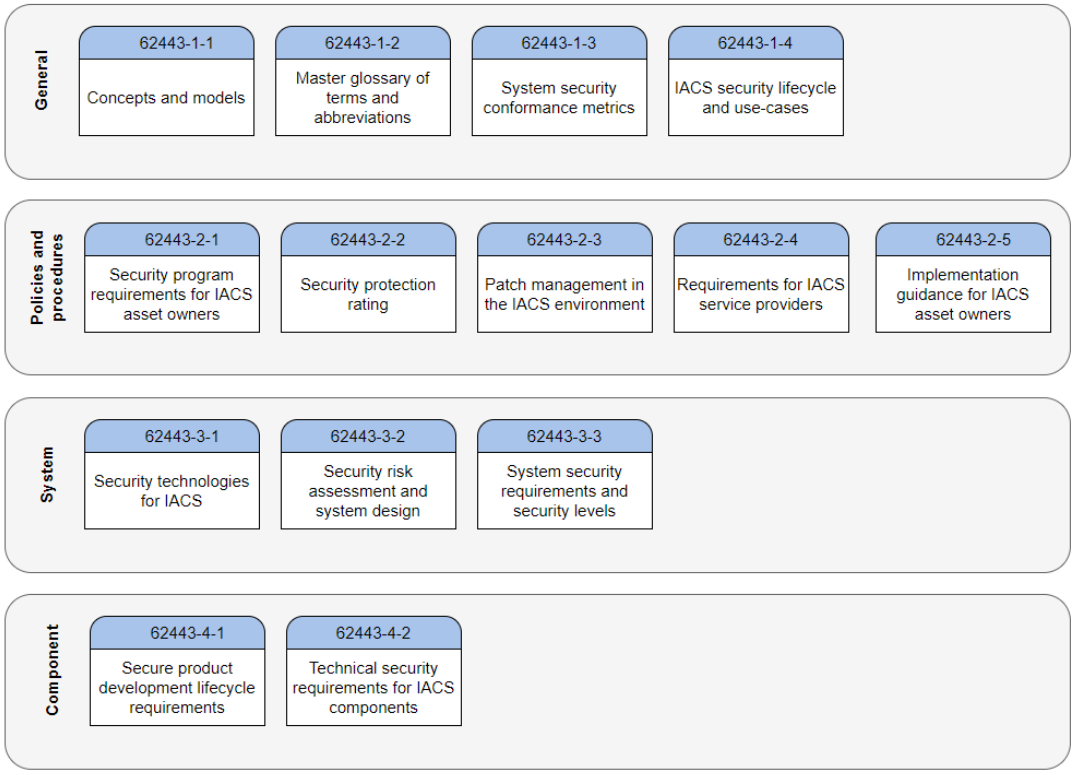

Figure 11. IEC 62443 different parts [19]

As we can see from the figure the IEC 62443 standards are divided into four levels: general, policies and procedures, system and component level. The standards include technical reports and technical specifications.

The IEC 62443 standard series brings up some principles related to industrial systems and their cybersecurity. Defence in depth is a concept which means that several different layers of protection or security which are distributed across of the overall system will make the system more secure since there is redundancy in terms of security controls.

Another topic that comes up in IEC 62443 standard series is zones and conduits. Zones and conduits are a way of representing a system. Zones are groups of assets that are similar in terms on security requirements. Conduits then are the way of connecting different zones and they make the communication between zones possible.

5.3 Network segmentation

The ISO/IEC 27001 standard [30] has one control for network segregation under the category of network security management and it says that information services, users and information systems should be segregated.

The IEC 62443-2-1 [23] has an example reference architecture alignment with an example segmented architecture. The system is segmented into different zoned that are: control zone, DMZ and business/enterprise zone. The standard states that for low risk IACS, the network segmentation might not be necessary but for medium and high risk IACS systems segmenting the network is a proven way of reducing the risks.

The IEC 62443-4-2 [28] also mentions network segmentation, but it is more on the component level instead overall cyber security management level. Something like access from world wide web to the control systems must be considered with the requirements of the system when connecting OT systems with IT.

When considering the ISO/IEC 27001 and IEC 62443 standards' guidance for an IT/OT converged system for network segmentation the overall system could look like the example in the Figure 4 earlier in this thesis. The figure does not have a DMZ in it, but it could fit between the OT networks and IT network.

5.4 Cryptography

Cryptography is generally used a lot in IT systems like, for example, encrypted password stored to a database. Cryptography helps to protect the integrity of the data. Converged systems with IT/OT also require cryptography if the data transferred is something that

could be used by an adversary to cause harm. Cryptography practises include, for example, using a strong encryption method and having a proper generator for cryptographic keys.

The ISO/IEC 27001 standard [30] covers some cryptography related cybersecurity practises. It has two controls for cryptography that are policy on the use of cryptographic controls and key management.

The IEC 62443-4-2 [28] standard has requirements for component level and one of them is use of cryptography. The requirements mentions that advanced encryption standard AES and secure hash algorithms (SHA) series should be used. It also mentions that when generating keys, a proper and effective random number generator should be used.

5.5 Incident management

Reacting to cyber incidents in an environment where IT and OT are converged is quite challenging if the incident targets a part of system where it affects both IT and OT. If the OT and IT systems were separated, they would probably react and manage cybersecurity incidents quite differently. With a converged system a coherent incident response and management is also needed.

The ISO/IEC 27001 standard [30] has a group of controls for information security incident management. It lists seven different controls for information security incident management. Here are the relevant controls from the list: reporting information security events and weaknesses, assessing events, responding to incidents, and learning from incidents. Learning from incidents is a good one since information security and cybersecurity as a whole is a constant process and learning from incidents is a big part of this so that it is easier to prevent the future incidents.

The IEC 62443-4-2 [28] has requirements for incident response. It requires that there is a team that responses to the incidents according to certain procedures. Reacting to cyber incidents is a big part of the whole incident management. Overall, the incident response to systems within OT is quite difficult and different from IT and that is why the better approach is usually to focus on preventive incident management.

5.6 Operations security

The ISO/IEC 27001 [30] standard has 14 controls for operations security under 7 different subcategories. Operations security is an interesting part of the ISO/IEC 27001 standard when considering the IT/OT converge and most interesting subcategories are: backups, and logging and monitoring.

The standard has one control for backup, and it is about information backups. It brings up recovery controls as a security practise in case of malwares. The ability to recover systems is especially relevant for OT systems where downtime is more serious than in IT systems like said earlier.

For logging and monitoring ISO/IEC 27001 [30] has 4 different controls that are: event logging, protection of event logging, administrator and operator logs and clock synchronisation. Logging events is also very relevant for IT and OT systems and specially when they are connected since that increases the numbers of subsystems in the overall system by quite a lot.

The IEC 62443 standard series has similar requirements and practises as the ISO/IEC 27001 for operational security. The IEC 62443-3-3 [26] has requirements on a system level for logging for different systems by the control system.

IEC 62443-4-2 [28] has similar requirements as 62433-3-3 [26] but on component level. The standard mentions about how components should be able to generate audit records for several different categories such as access control, backups and request errors.

The IEC 62443-4-2 [28] also includes in-depth guidance on component level for backups and recovery. It has an own requirement for control system back-up and recovery. The standard guides that the components should also be able to be part of the backup process and how the backups must not affect the operations of components. Also, another important practise is the ability to recover into a safe state after failure or disruption.

Being able to monitor on the system level and the component level is important and makes tracking the changes and potential problems in the overall system a lot easier. This is something that becomes easier with more connectivity. OT systems have generally been isolated and also been harder to monitor. Connectivity with IT systems makes the ability to monitor OT systems smoother and easier. Another benefit is the ability to do maintenance or backups and recoveries for the devices with remote control. If OT systems would be isolated all the maintenances and work done with them would most likely have been done by hand with physical presence.

5.7 Access control and authentication

The ISO/IEC 27001 standard [30] has 14 controls for access controls category in 4 subcategories. The different subcategories cover topics for: business requirements of access control, user access management, user responsibilities and system and application access control.

Managing remote access is important when IT and OT system are converged. Being able to authenticate users accessing the system remotely is important. IEC 62443-2-1 [23] has a sub annex for “authentication for remote users”. The annex mentions that industrial operations where health and safety are at stake strong authentication technologies should be used. This applies to railway systems as well so a weak authentication method such as a simple used ID and password is not enough. The IEC 62443-2-1 [23] standard also recommends that the remote users are not allowed to control the system but only monitor.

The IEC 62443-3-3 [26] standard has a lot of requirements towards authentication and identification. In the IEC 62443-4-1 [27] and IEC 62443-4-2 [28] there are similar requirements but on a component level. There are several requirements that are relevant for IT/OT converged system. For example: Account management, authenticator management, wireless access management. It also has different password related requirements. The IEC 62443 standard series covers authentication and access control in IACS environments quite broadly and detailed.

5.8 Patch management

As said in the chapter 4 patch management is crucial for IT/OT converged systems and IT and OT have had highly different processes for patching. When isolated OT systems might go several years or even decades without any patches while IT systems get regular patches.

The ISO/IEC 27001 standard [30] does not have any guidance or controls for patching policies, but the IEC 62443 standard series has a whole standard for patching: IEC 62443-2-3 [24] Patch management in the IACS environment. The IEC 62443-2-3 [24] covers the patch management as whole and the different aspects of it. It has guidance for the patch management as a process from the planning phase to the monitoring and testing and all the way to the patch deployment and installation. Patch management is a practise that has to be adapted to the OT world with the increasing connectivity.

6. RESULTS

This chapter includes the results of studying the three cybersecurity standards in the context of Digirail. This chapter aims to answer the research question of this thesis about how well the TS50701 standards includes guidance for IT and OT and what topics need additional guidance from ISO/IEC 27001 and IEC 62443.

This chapter starts with by going through the interviews and their results. Interviews are gone through by one question at a time and the most interesting and relevant answers that came up are presented.

The cybersecurity practises are gone through with the two previous chapters. The interviews and other possible materials are also referred and used to analyse the standards according to Digirail environment. The aim is to present which parts of each standard are relevant for each topic and could be used as a guidance. At the end there is an overview of the standards and some comparisons between the standards.

6.1 Interviews

The interviews had few questions prepared beforehand to guide the interview and help the interviewees with their answers. The following questions were prepared for the interviews. Other than the questions there is not a clear structure for the interviews. This is because the topic is quite open and strict questions would limit the potential topics that might otherwise come up during the interviews.

1. What are the most relevant parts of Digirail from OT and IT side?
2. What challenges does the converge of IT and OT bring for Digirail for IT and OT sides?
3. What needs are there for OT and IT to be converged? For example, what does OT need from IT and vice versa?
4. What OT and IT cybersecurity practises could be applied for Digirail IT and OT converge?

These questions were the guideline for the interviews, but they also focused based on the interviewee and their expertise.

There were four interviews in total and the interviewees had different backgrounds. That made the interviews somewhat challenging but also interesting since the interviewees

brought up different kinds of topic. The challenging part was trying to adapt the interview according to the interviewees and that is something that could have been planned better beforehand. Overall, the interviews were beneficial for writing this thesis and they helped to bring up new points and topics. The results of the interviews are covered in the results chapter.

6.1.1 Results to the questions

Q1: What are the most relevant parts of Digirail from OT and IT side?

The topic that was most brought up from this question was the RBC-interlocking interface. RBC and interlocking are a central part of the Digirail environment. RBC is one of the biggest differences when changing to the ERTMS system and if the RBC and interlocking are part of the same entirety must be determined.

RBC and interlocking are more of the OT side of the overall system. OT side is more vulnerable and concerned with safety and not just security. IT side is less critical since the railway environment's cybersecurity is related to safety and securing the OT equipment is crucial to prevent physical harm.

Other topics that were brought was, for example, the communication network with the upcoming FRMCS and how crucial it is. Changing the communication to wireless system and possibly using public networks creates challenges and risks that need to be addressed. There is a need for good overall architecture presentation of the network and not just the physical one but a logical one which shows the actual connections form the security perspective.

Q2: What challenges does the converge of IT and OT bring for Digirail from IT and OT sides?

One of the topics that was brought up on this question is how all the IT and OT assets and their vulnerabilities can be recognised. Also, all the different interfaces and zones and how can they be used for attacks was brought up.

Another challenge that came up is the lifecycle on different devices and how cybersecurity has been implemented into them. OT devices usually have not done this properly so converging them with IT is a big challenge. Patch management is also a challenge since OT requires uptime. OT devices might also lack on certain aspects like authentication and access control and, for example, there might only be one admin credentials which are used for authentication. A centralised access control for OT environment is needed.

IT world is generally faster and agile than OT and it has more computing power. OT is slower and might not be compatible with everything that IT can offer. This creates challenges since OT is more focused on operativity than speed.

Q3: What needs are there for OT and IT to be converged? For example, what does OT need from IT and vice versa?

Topics that were brought up: ability to collect data for maintenance and better ability to react to incidents. For example, IT systems enable automatic reactions to certain situations. Hence OT needs monitoring and data collection possibilities from IT and thus enabling better maintenance.

Ability to use Internet Protocol (IP) networks and IP in general is a benefit that comes with Digirail. IP makes it is easier to use and integrate IT devices since they generally are compatible with IP.

Q4: What OT and IT cybersecurity practises could be applied for Digirail IT and OT converge?

There were some topics that came up for this question. For example, bringing patch management practises from IT applies to Digirail as well. Practises like authentication and key management are also applicable for Digirail IT/OT conversion.

Whitelisting was mentioned as a more detailed practise. Whitelisting works better for OT since the programs rarely change. This allows to only whitelist the necessary programs which can prevent malwares of having an impact.

6.1.2 Additional results

There were some additional topics that came up during the interviews that weren't directly related to any of the questions:

Generally, with IT/OT converge things are more moving from IT to OT. So that means more of the practises and features of the IT world are more useful in general. IT has been developed better to handle cyber threats and these measures can be applied to OT world.

6.2 Best OT and IT cybersecurity practises for Digirail

In this sub-chapter the cybersecurity practises from TS50701 are reviewed in the context of Digirail environment. TS50701 is compared to the IEC 62443 and ISO/IEC 27001 to see how well it covers different topics and how well it suits as guidance for Digirail. The practises are gone through by the same or similar categories as the previous chapters.

6.2.1 Network segmentation

Network segmentation is mentioned as a good cybersecurity practise for OT systems in several sources [3] [34]. RazorSecure has an article for network segmentation for railway environment [43]. In the article it is mentioned that segmentation is difficult in an environment like railways.

In Digirail as a whole there are a lot of different subsystems and in railways in general there are moving trains and it is called rolling-stock system. Network segmentation is generally widely used in IACS systems and systems are usually divided into different zones. The interviews also brought up the zones and their interfaces as a topic that relates to Digirail a lot and as something that needs to be considered.

As stated in chapter 4 the TS50701 [11] document has guidance for network segmentation. In the restricted flow section Foundational Requirement (FR) 5 of the requirement table there are requirements related to network segmentation. The requirements are referred from the IEC 62443-3-3 [26] requirement table. The TS50701 also refers to the IEC 62443-4-2 [28] standard and states that business assets (IT) should be separated from the control assets (OT). TS50701 [11] also has several other guidelines related to network segmentation under the section restricted data flow.

The requirement mentioned earlier has an additional railway related information that is very relevant for Digirail as well. It states that incident situations are something that must be handled in a way that the operations can continue. The document mentions that, for example, some connections between different network segments might have to be broken in case of an incident. Standard brings up practises like duplicating control system network in case something needs to be shut down due to an incident.

The IEC 62443-4-2 [28] includes guidance on component level for network segmentation. It mentions about the differences of logically and physically segmenting a network. Physically segmented networks provide a better layer of security over logically segmenting. The physical segmentation requirement is also referenced in the TS50701 [11] and it includes additional railway related information that a logical segmentation can be used if physical is not possible.

Network segmentation is a cybersecurity practise that is generally mentioned when talking about OT or IACS systems and not so much with just pure information systems. When connecting OT with IT system the segmentation becomes more relevant. This is relevant for Digirail as, for example, the train control systems in the train must be segmented in a way that they cannot be used to access public world wide web because that might lead to malicious executable files getting downloaded to the computers running the train control systems. The train, however, must be able to communicate with the track side systems, so the segmentation has to be planned and implemented properly. As stated in the interviews RBC and interlocking are central part of the operation in Digirail so the network should be segmented so that they are protected properly.

The TS50701 standard [11] gives great overall guidance on network segmentation for railways environments and it could be used for Digirail as well. Even though network segmentation can generally be thought as a cybersecurity practise for OT which is more relevant for Digirail than IT network segmentation. The ISO/IEC 27001 does have guidance for the topic as well. Like mentioned in the chapter 5 of this thesis ISO/IEC 27001 does have control for segregating the users, systems and services for IT systems.

6.2.2 Cryptography

Cryptography is important in general and also for Digirail environment. The TS50701 [11] document has a system requirement SR 3.1 for cryptographic integrity protection, and it has reference to the IEC 62443-3 standard. The requirement has an additional note for railways that highlights the importance that the cryptographic measures are secure. It also mentions about open and untrusted networks and that they need extra protection in railways. This is relevant for Digirail and future of railways. The potential of using open networks for communication in ERTMS systems requires better cryptographic environment than a closed for instance private network would.

These cryptographic measures could, for example, mean the use of better encryption methods such as AES instead of using vulnerable ones like DES or no encryption at all. The TS50701 [11] does not however mention key management as a requirement but as stated in the earlier chapter the ISO/IEC 27001 standard [30] has a requirement for key management for cryptographic controls. Cryptographic keys and key management system could be an important factor of making the communication between different assets in the Digirail environment secure.

Topic that came up from the interviews is that some of the OT devices might not be compatible with all encryption methods and algorithms which might limit the potentially usable methods for encryption.

Figure 12 [35] shows an example of how cryptography tools from IT and OT worlds can work together in an energy system.

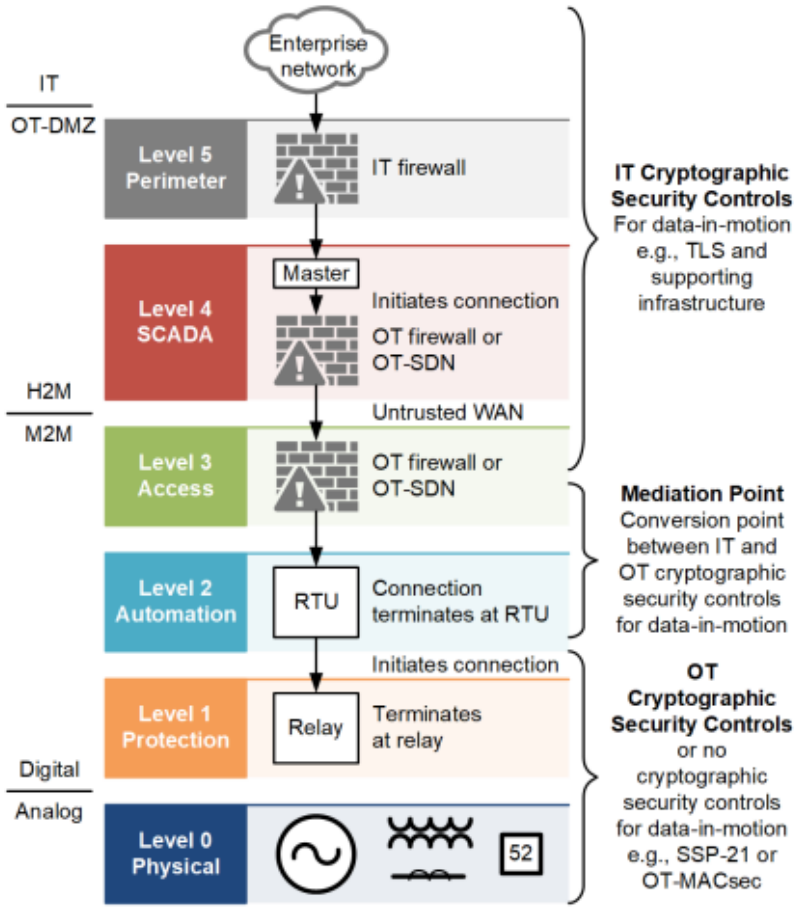

Figure 12. IT cryptography and OT cryptography in an energy system [35]

Similar kind of architecture could be studied for Digirail where the cryptography practises and protocols from IT and OT could be used together in a system.

Overall the TS50701 gives great guidance on cryptography with railway related notes but the IEC 62443 could be used as additional guidance for Digirail since it gives more guidance especially on the component level and more detailed guidelines, for example, about different algorithms like SHA and AES. The guidance on cryptography from the ISO/IEC 27001 is quite limited and not in depth and for example IEC 27002 standard could be used as an additional source for guidance on this topic.

6.2.3 Authentication and access control

With Digirail the Finnish railway environment is going to change quite a lot. With the addition of ERTMS as the new traffic management system that uses wireless communication, authentication and access control become more relevant. Authentication and access control are cybersecurity practises that are widely used in different environments.

Enisa lists [42] software process and device identification and authentication as an example practise against the scenario 1 example attack listed in chapter 2.3 of this thesis. In the same document human user identification and authentication are also mentioned as one example practise against scenario 4. These are examples of how big impact a good authentication and access control can have on the overall cybersecurity.

The TS50701 standard has several requirements listed for authentication which are derived from the IEC 62443-3-3 [26] standard. The standard has a lot of requirements under the “Identification and authentication control” category. One of the best practises in terms of authentication that is widely used nowadays is multifactor authentication and it is defined in the standard. It is defined separately for trusted and untrusted networks. Multifactor authentication solution is generally used in the IT world, but it could be applied to the railway world. The TS50701 document [11] mentions phone calls as an example way of recognizing the human users.

The Digirail environment has a lot of different component and different processes. The different components need to be able to authenticate with each other. This becomes especially relevant with the context of OT/IT converge since the OT devices become more vulnerable. The TS50701 [11] has a requirement for “Identification and authentication of software processes and devices” and it mentions that railways identifications are not usually used for internal software and processes in railway world. This is true but the identification for software processes as well will become relevant in the future.

One factor that becomes especially relevant with Digirail and its IT and OT systems is wireless access management. The interviews highlighted the importance of interlocking and the different interfaces it has. Remote managing the interlocking, for example, from traffic control is something that needs proper authentication and access control methods. Being able to wirelessly connect to OT systems requires protection and the TS50701 [11] has a requirement for managing wireless access management and it is based on the IEC 62443-3-3 [26] standard. It has no additional information for railways.

Passwords is a subject that has been quite differently handled in IT and OT worlds. A lot of OT systems and devices might have used simple password or a default password for a long time but since OT systems are not going to be isolated anymore the password

policies also need to change. And on the other hand, IT systems usually require strong passwords that need to be changed from time to time. The TS50701 has requirements related to password strength and password lifetimes that could be applied for Digirail.

Overall TS50701 has very good guidance on authentication and access control since it has several different requirements from the IEC 62443 series with additional railway information added. Access control and authentication is a topic that is well covered in all the three standards.

6.2.4 Patch management

Patch management is a practise that has been very different in IT and OT environments. IT generally has scheduled and regular patches and OT on the other hand could go years without patching the system or device a single time. When IT and OT become connected the good patch management practises from IT should be adapted into OT as well.

TS50701 [11] has a whole subclause 10.3 about guidance for patch management. IEC 62443-2-3 is a whole standard dedicated for patch management and the TS50701 does refer to that standard, for example, with how patch testing process should be done.

The IEC 62443-2-3 [24] brings up the downsides and impacts of having a poor patch management. It could, for example, make the system vulnerable and unstable and without a proper patch management system the patches might not be compatible with control systems and their software. The standard gives great guidance of how to patch process should be handled and, for example, how the patch information should be handled and transferred.

When working with industrial systems, the patching and the uptime of the system has to be kept in mind. Like covered earlier the TS50701 does have guidance for patching while ensuring that the operational requirements are not scattered. TS50701 [11] guidance on patch management can be used for Digirail but the IEC 62443-2-3 is [24] definitely also relevant since it is a whole standard dedicated for patch management.

6.2.5 Backups and recovery

Backups and recovery have been used on both on IT and OT environments. Backups and recovery could be used for data or systems. For railways and Digirail the most important is surely the ability to backup systems and if necessary to recover systems so that the uptime can be continued. Enisa report about railway security [42] has an exam-

ple cyberattack scenario – Disastrous event destroying the datacentre, leading to disruption of IT services. Parts of the TS50701 standards about control system recovery and backups are mentioned as a security measure for this attack.

As covered earlier in chapter 4 TS50701 [11] does have guidelines for backups in railway environment. It has, for example, a requirement that is referenced from the IEC 62443-3-3 standard for control system backup. For that requirement it has additional railway related information about how critical files and files should be able to be backed up.

Digirail environment requires that backups are able to be done to both the IT and OT systems and same goes for recoveries. It is crucial that the uptime of the OT systems is maintained as mentioned in the interviews as well. The part “Resource availability” from the cybersecurity requirements table from TS50701 [11] has a lot of guidance for backups and recoveries in railway environment.

Overall, the TS50701 [11] has good guidance for backups and recovery under the FR 7 section. It is not quite so detailed so IEC 62443 and ISO/IEC 27001 could be used for additional guidance for Digirail.

6.2.6 Incident management

Reacting to incidents is important cybersecurity practise. Incident or cyber incident is quite a broad matter and hard to precisely determine. National cyber security centre defines cyber incident [52]: “a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems”.

Like many of other practises it has been generally different in the worlds of OT and IT. OT has usually been more focused on preventive security and reacting to incidents has been difficult. IT on other hand has had better tools for shutting down systems or connections in case of an attack or other incident.

The TS50701 standard [11] states that on the current version of the standard incident management is not included and will be addressed on later versions of the standard. Guidance for incident management for IT and OT sides can be found from the IEC 62443 and ISO/IEC 27001 standards. ISO/IEC 27001 [30] has 7 controls for Information security incident management. IEC 62443-2-1 [23] has guidance for incident management on a policy level but there is not really any guidance on a more operative level on an OT environment like railways. Incident management is a topic that should be studied further to find out if there is potential guidance that could be used.

6.2.7 Other topics

Other relevant practises for IT/OT converged system that could be useful for Digirail are for example malicious code protection. In the Enisa document [42] they mention malicious code protection and software and information integrity as countermeasures against for example a ransomware attack.

In TS50701 [11] there is a requirement for that practise, and it mentions that use of USB ports should be considered and limited. USB ports are known to be threat for industrial and automation systems and there has been malware that have infected system through USB ports.

Other interesting topics from ISO/IEC 27001 [30] that were not covered earlier in this thesis would be for example human resource security. Humans are often the weak link in terms of cybersecurity and making sure humans are as prepared as possible for cybersecurity is a good practise. Protection against malware is also an interesting control that can be found from ISO/IEC 27001 and could be useful for Digirail. With increasing IT/OT converge the possibility that malwares could infect OT devices also increases.

6.3 Overview of cybersecurity practises and standards

In general, the TS50701 gives great guidance for several different areas of cybersecurity practises. A lot of the cybersecurity requirements and guidelines from TS50701 standard are referred to the IEC 62443 standard series. They do, however, have good railway specific information. Even though general cybersecurity guidance can be used for Digirail, railway related guidance is always relevant and thus the value of TS50701 standard is high. The Digirail environment is a bit different from a generic automation or industrial system so following only the IEC 62443 standard is obviously harder than using the railway specific guidance from TS50701.

Table 4 shows overview of the different standards and the different practises. The most relevant parts of the standards can be seen from the table. The TS50701 column shows how well the topics and practises are included and guided in the standard. The IEC 62443 and ISO/IEC 27001 columns show what parts could be used to complement the TS50701 standard from OT and IT sides respectively.

The table is also colour coded to give an idea of how well the standards give guidance of each topic. Green means it is covered well, orange that it is covered but lacks in certain aspects and red that it is not covered at all or very little.

Table 4. Overview of the cybersecurity standards

	TS50701	IEC 62443	ISO/IEC 27001
Cryptography	SR 3.1 and SR 4.3	CR 4.3 (4-2) and SR 4.3 (3-3)	A.10
Incident management	Not included	Table 17 (2-1)	A.16
Network segmentation	FR 5	FR 5 (3-3)	A.13.1
Patch management	Subclause 10.3	Standard 62443-2-3	Not included
Backups and recovery	SR 7.3 and SR 7.4	SR 7.3 and SR 7.4 (3-3)	A.12.3
Authentication and access control	FR 1, parts of FR 2	FR 1 (3-3) and clause 5 (3-1)	A.9

Topics that are well covered in the TS50701 standard are shown in green in the table. They are authentication and access control, and network segmentation. These are topics that do not necessarily need additional guidelines from the other standards. These are also important topics for OT systems and on the ENISA document they mentioned about cybersecurity measures and that for OT the emphasis is on security network segmentation and access control [42].

Topics that are covered but could use additional guidance from other standards are shown in orange and they are backups and recovery, patch management and also cryptography. These are topics that have good guidance on the TS50701 alone but could use more detailed or larger guidance that could be looked for from the IEC 62443 and ISO/IEC 27001 standards.

Topic that is not included at all is shown in red and it is incident management. We can see that incident management is not green on any of the standards so that means it should be studied further from potentially other sources and make a guidance for Digirail.

6.4 Comparing the standards

The IEC 62443 and ISO/IEC 27001 are more general standards whereas TS50701 has a lot of railway specific guidance. The IEC 62443 is the largest of the three standards since it composes of several different standards. It also has detailed information, for example, about authentication since it introduces several different authentication methods. The IEC 62443 could be used for studying the topic more detailed even though TS50701 already has very good guidance on that.

The TS50701 largely overlaps with IEC 62443 since it is heavily based on it. The requirements are similar and the structure of the document is also very similar. The biggest difference between the standards is that TS50701 is railway specific and IEC 62443 more general standard. The system requirements on the TS50701 are derived from IEC

62443-3-3 and most of them have railway related additional information. Only topic that does not have any railway specific information on any requirements is “Timely response to events” (TRE) which contains requirements for logging and monitoring. All off the topics in Table 4 have additional railway guidance so they are just not plain references to the IEC 62443 standard.

ISO/IEC 27001 is the shortest of the three standards and the one with least detailed information. Other standards from the IEC 27000 series like the IEC 27002 standard could be studied for more guidance on the IT side. The IEC 27002 is also referred a lot in the Enisa document [42] for different measures and practises so it could be useful for railways.

7. CONCLUSIONS

With the findings presented in chapter 6 the TS50701 standard can be considered as a quite well-made standard that covers a lot of important topics for railway cybersecurity. It is a new standard and that is why it is natural that not all topics are covered like incident management There will be updated versions of the standard in the future that will become more in depth. Just like cybersecurity in general the standards for it are in a constant cycle and they need to stay up to date with the latest changes in cybersecurity. Cybersecurity is becoming more relevant for railways, and it is important to have proper guidance like the TS50701 standard for it.

The IEC 62443 and ISO/IEC 27001 are overall good and inclusive cybersecurity standards from IT and OT point of views. They are obviously not railway specific and that is why not all of the guidelines are suitable for railways directly at least on very detailed level. A higher-level guidance can be adapted from the IEC 62443 and ISO/IEC 27001 as well.

This thesis gives guidance for the coherent management of the overall cybersecurity that involves both IT and OT by finding the best parts of the different standards for IT and OT. This thesis finds the most relevant parts of the three standards for the specific topics that are relevant for the IT/OT converge. Other topics like human interaction could be studied from the standards to see how well the guidance fits for Digirail. Incident management could also be studied further since the guidance on it is quite limited on the three standards. This thesis gives only theoretical results and so the next steps could be studying how to apply the best cybersecurity practises from the standards into real environment.

The thesis succeeded in finding the relevant parts of the standards but, however, the restriction on the topic could have been done better. For example, there could have been only certain aspects or certain cybersecurity practises to focus on from the start. The focus points on the practises came along the way of making the thesis but having certain practises to focus right from the beginning would have made the thesis writing process smoother.

Railway and transportation sector in general is quite critical and digitalization definitely brings new benefits to it and enhances the operation. It also brings new risks and topics that were previously almost ignored are now important. Aspects like cyber warfare could greatly affect railways by, for example, shutting down the railway systems. It is important

that railway world keeps up with cybersecurity and different guidance and instructions are needed and will be needed in the future.

REFERENCES

[1] A. Härkönen, L. Aarnio, J. Mantsinen, J. Neuvonen, T.Hulkko, ERTMS/ETCS-tason 2 junien kulunvalvontajärjestelmän toteutusvaihtoehdot Suomessa, Finnish Transport Infrastructure Agency, November 2021, Available: https://www.doria.fi/bitstream/handle/10024/180703/vj_2021-16_978-952-317-852-6.pdf?sequence=1&isAllowed=y

[2] A. Teuling, S.Liethoff, E. Koning, M.Jutte, B.Feskens, Implications of OT and IT Integration for Cyber Security, HSD securitydelta, 2020 (Updated 2021) Available: https://securitydelta.nl/media/com_hsd/report/403/document/HSD-Rapport-OT-mei-2021.pdf

[3] B. Czarny, Best Practises for ICS and OT Security, Security Boulevard, September 2021, Available: https://securityboulevard.com/2021/09/best-practices-for-ics-and-ot-security/

[4] B. Lutkevich, DMZ in networking, TechTarget, July 2021, Available: https://searchsecurity.techtarget.com/definition/DMZ

[5] B. Lutkevich, Patch Tuesday, Techtarget, September 2021, Available: https://www.techtarget.com/searchsecurity/definition/Patch-Tuesday

[6] C. Bogen, Bridging the Gap Between IT And OT Cybersecurity, T&D World, May 2019, Available: https://www.tdworld.com/smart-utility/grid-security/article/20972635/bridging-the-gap-between-it-and-ot-cybersecurity

[7] C. Cimpanu, DDoS Attacks Cause Train Delays Across Sweden, Bleepingcomputer, October 2017, Available: https://www.bleepingcomputer.com/news/security/ddos-attacks-cause-train-delays-across-sweden/

[8] C. Coy, M. Gadbois, Connectivity & Cyberscurity part 1 of 3 IT-OT convergence, Automation.com, February 2021, Available: https://www.automation.com/en-us/articles/february-2021/connectivity-cybersecurity-1-it-ot-convergence

[9] C. Kakilla, Strengths and Weaknesses of Semi-Structured Interviews in Qualitative Research: A Critical Essay, ResearchGate, June 2021, Available: https://www.researchgate.net/publication/352565661_Strengths_and_Weaknesses_of_Semi-Structured_Interviews_in_Qualitative_Research_A_Critical_Essay

[10] Choosing an Interview Type for Qualitative Research, Statistics Solutions, Available: https://www.statisticssolutions.com/choosing-an-interview-type-for-qualitative-research/

[11] CLC/TS 50701 Railway applications, Cybersecurity, CENELEC, 2021

[12] Cyberattack hits Danish rail network, The Local DK, May 2018, Available: https://www.thelocal.dk/20180514/cyber-attack-hits-danish-rail-network/

[13] Cyber-attack hits Iran's transport ministry and railways, The Guardian, July 2021, Available: https://www.theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways

[14] Cybersecurity in Operational Technology: 7 Insights You Need to Know, Ponemon Institute, March 2019

[15] Cybersecurity in the Railway sector - D2.1 – Safety and Security requirements of Rail transport system in multi-stakeholder environments, Cyrail, June 2017

[16] D. Kushner, The Real Story of Stuxnet, IEEE Spectrum, February 2013, Available: https://spectrum.ieee.org/the-real-story-of-stuxnet

[17] D. Liveri, M. Theocharidou, R. Naydenov, Railway Cybersecurity: security measures in the Railway Transport Sector, ENISA, November 2020, Available: https://www.enisa.europa.eu/publications/railway-cybersecurity

[18] D. Walkowski, What is the CIA Triad, F5labs, July 2019, Available: https://www.f5.com/labs/articles/education/what-is-the-cia-triad

[19] E. Cosman, Structuring the ISA/IEC 62443 standards, ISA, Available: https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards

[20] E. Perkins, Operational Technology Security – Focus on Securing Industrial Control and Automation Systems, Gartner, March 2014, Available: https://blogs.gartner.com/earl-perkins/2014/03/14/operational-technology-security-focus-on-securing-industrial-control-and-automation-systems/

[21] F. De Peralta, M. Watson, R. Bays, J. Boles, F. Powers, Cybersecurity Resiliency of Marine Renewable Energy System Part 2: Cybersecurity Best Practises and Risk Management, Pacific Northwest National Laboratory, April 2021

[22] I. Lopez, M. Aguado, Cyber security study of the European Rail Traffic Management System, Researchgate, February 2016, Available: https://www.researchgate.net/publication/301636052_Cyber_security_study_of_the_European_Rail_Traffic_Management_System

[23] IEC 62443-2-1 Industrial communication networks. Network and system security. Part 2-1: Establishing an industrial automation and control system security program, 2013

[24] IEC 62443-2-3 Security for industrial automation and control systems- part 2-3: Patch management in the IACS environment, 2015

[25] IEC 62443-3-1 Industrial communication networks. Network and system security. Part 3-1: Security technologies for industrial automation and control systems, 2013

[26] IEC 62443-3-3, Industrial communication networks. Network and system security. Part 3-3: System security requirements and security levels, 2019

[27] IEC 62443-4-1, Security for industrial automation and control systems. Part 4.1: Secure product development lifecycle requirements, 2018

[28] IEC 62443-4-2 Security for industrial automation and control systems. Part 4.2: Technical security requirements for IACS components, 2019

[29] ISO/IEC 27001 Information Security Management, ISO, Available: https://www.iso.org/isoiec-27001-information-security.html

[30] ISO/IEC 27001:2017, Information technology. Security techniques. Information security management systems.

[31] IT - OT convergence The future of digital railways might hinge on the rise of asse management, ABB, Microsoft, Available: library.e.abb.com/public/03877e7e6cf848faa056787207e69d02/IT-OT%20rail%20survey_A4_9AKK106930A9099_170906.pdf

[32] IT and OT convergence – two worlds converging in Industrial IoT, I-Scoop, Available: https://www.i-scoop.eu/internet-of-things-iot/industrial-internet-things-it-ot/

[33] IT vs OT security: The Operational Technology Guide For Professionals, Otorio, September 2020, Available: https://www.otorio.com/blog/it-security-vs-ot-security-the-operational-technology-cybersecurity-guide-for-industry-professionals/

[34] J, Caraballo, Operational Technology (OT) Cybersecurity 4 Best Practises, BeyondTrust, April 2021, Available: https://www.beyondtrust.com/blog/entry/operational-technology-ot-cybersecurity-4-best-practices

[35] J. Carlson, D. Gunter, C. Roberts, C. Gordon, G. Masters, Do IT Cryptographic Controls Work for Energy Systems, SEL, April 2021 (Updated May 2021), Available: https://selinc.com/mktg/134007/

[36] J. Pylvänäinen, J.Lehtola, L.Toivakka. J. Westerling, V. Tervola, A. Tiilikainen, M. Brotherus, L. Ahtiainen, J.Kuismin, Digirata- valmisteluvaiheen loppuraportti, Ministry of Transport and Communications, July 2021, Available: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163295/LVM_2021_17.pdf?sequence=4

[37] J.C. Sapien, Global Cyber Attack Hits Deutsche Bahn, Railway-News, May 2017, Available: https://railway-news.com/global-cyber-attack-hits-deutsche-bahn/

[38] K. Cameron, 4 Types of Access Control, Four Walls Security Blog, April 2020, Available: https://www.fourwallssecurity.com.au/blog/4-types-of-access-control

[39] M. Arora, How secure is AES against brute force attacks, EETimes, July, 2012, Available: https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/#

[40] M. Mattei, IT vs. OT Security: 6 Strategies You Can Adapt to Secure OT Environments, ModernCISO, Oct 2020, Available: https://modernciso.com/2020/10/01/it-vs-ot-security-6-strategies-you-can-adapt-to-secure-ot-environments/

[41] M. Smith, OT/IT network convergence: experience-based best practices, Process Technology, March 2020, Available: https://www.processonline.com.au/content/industrial-networks-buses/article/ot-it-network-convergence-experience-based-best-practices-752461501

[42] M. Theocharidou, Z. Stanic, L. De Mauroy, L. Lebain, J. Haddad, railway cybersecurity - Good practices in cyber risk management, ENISA, November 2021, Available: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management

[43] Network segmentation and segregation - an important cyber security principle for the rail industry, Razorsecure, Available: https://www.razorsecure.com/post/network-segmentation-segregation-for-the-rail-industry

[44] New ISA/IEC 62443 standard specifies security capabilities for control system components, ISA, Available: https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

[45] P. Katuzura, IT-OT Convergence: Managing the Cybersecurity Risks, Available: https://gca.isa.org/blog/it-ot-convergence-managing-the-cybersecurity-risks

[46] R. Bloomfield, M. Bendele, P. Bishop, R. Stroud, S. Tonks, The Risk assessment of ERTMS-based railway systems from a cyber security perspective: methodology and lessons learned, City University of London Institutional Repository, Available: https://openaccess.city.ac.uk/id/eprint/15105/8/Bloomfield2_ERTMS_RSSR2016.pdf

[47] Suositus kyberturvallisuuden edistämisestä raideliikenteessä, Traficom, July 2020, Available: https://www.traficom.fi/sites/default/files/media/regulation/Suositus%20kyberturvallisuuden%20edist%C3%A4misest%C3%A4%20raideliikenteess%C3%A4.pdf

[48] T. Cheshire, Four Attacks on UK Railways In A Year, Skynews, July 2016, Available: https://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558

[49] T. Chothia, M. Ordean, J. De Ruiter, J. Richard, An attack against message authentication in the ERTMS train to trackside communication protocols, Unitersity of Birmingham, 2017, Available: https://research.birmingham.ac.uk/en/publications/an-attack-against-message-authentication-in-the-ertms-train-to-tr

[50] Top 14 Data Security Best Practises, Netwrix, Available: https://www.netwrix.com/data_security_best_practices.html

[51] Ukraine power cut “was cyber-attack”, BBC, January 2017, Available: https://www.bbc.com/news/technology-38573074

[52] What is a cyber incident, National cyber security centre, September 2016 (updated November 2018), Available: https://www.ncsc.gov.uk/information/what-cyber-incident

[53] Z. Kleinman, Rail station wi-fi provider exposed traveller data, BBC, March 2020, Available: https://www.bbc.com/news/technology-51682280