Measures Needed to Integrate Physical and Cyber Security in Railways Infrastructure: Organization X Case Study

Pacelli Q. Felix Wagner, Yusuf M. Hussein

2021 Laurea

Laurea University of Applied Sciences

Measures Needed to Integrate Physical and Cyber Security in Railways Infrastructure: Organization X Case Study

P. Q. Felix Wagner, Yusuf M. Hussein
Safety, Security and Risk Management
Bachelor's Thesis
October 2021

Laurea University of Applied Sciences **Abstract**
Safety, Security and Risk Management
Bachelor of Business Administration

Pacelli Q. Felix Wagner, Yusuf M. Hussein

Measures Needed to Integrate Physical and Cyber Security in Railways Infrastructure: Organization X Case Study

Year 2021 Number of pages 41

Technological innovations, digitalization, and the increasing adaptation of IoT components into mass transportation networks worldwide have created new so-called converged security threats for the railway industry's overall security posture. In collaboration with our thesis' partner (SAFETY4RAILS project), the primary purpose of this study is to provide solutions to enhance the security and safety of railway operations. This study aimed to highlight the measures needed to assist Organization X and its members in converging physical and cybersecurity departments to improve their ability to identify, mitigate, and protect against emerging threats.

The method used to conduct the study was an exploratory research design, a qualitative data collection approach that comprised a literature review and a semi-structured qualitative interview, and a content analysis methodology to examine the results. We chose this structure flow because it offered the most refined research methodologies for obtaining important insights linked to Organization X and its members' current needs to integrate their cyber and physical security frameworks.

The results show that there is no one-size-fits-all solution to the convergence of physical and cybersecurity. Broad guidelines are required to handle security convergence issues such as corporate security structure with siloed teams, departmental cultural differences, employees' skills gaps, and probable discrepancies between business goals and security strategy.

Based on our findings, we conclude that to design and implement successful and effective cybersecurity and physical security convergence in the railway operations of Organization X's members, the three core areas of these organizations, namely people, process, and technology, must be seamlessly integrated.

Keywords: physical security, cybersecurity, railway security, measures for convergence

Contents

1 Introduction

The advancement of technology in the last decades and the increasing digitalization of mass transportation systems have created new challenges for implementing a safe, reliable, and efficient integration between cybersecurity and physical security environments in railways. According to Rekik, Gransart & Berbineau (2018), the increased dependency of railway systems in automation and information communication technologies (ICT) introduced new vulnerabilities to the threat landscape. Pizzi (2019) points out that railway transport has become deeply dependent on embedded systems. While doing risk analysis, the vulnerabilities found in such systems should be treated similarly to any other type of hazard to enhance railways' security environment.

The railway network service comprises various intertwined processes, which connects systems, applications, and infrastructures. Cyber-Physical systems are integrated environments where networks and systems can interact and control the physical domain (Yaacoub, Salman, Noura, Kaaniche, Chehab & Malli 2020). Transportation Cyber-Physical Systems (TCPS) is a modern transportation system that can provide a faster and more efficient cooperative response from cyber and physical systems in the transportation infrastructure. TCPS is an essential infrastructure for the daily function of society, and it englobes systems for a variety of purposes such as maritime, road and rail transportation. (Deka & Mashrur 2018.)

In the European Union (EU), the railway sector is responsible for an essential part of the economy from the member states. Serving approximately 472 billion passenger kilometres, 430 billion tonne kilometres for goods transportation, and having a comprehensive rail network operating in an extension of 216,000 kilometres, makes the railway network a vital infrastructure for the development and growth in the EU area (Eurostat 2020). With such interconnected processes and systems operating on TCPS, the increase in security risks and the surface the attacks can be deployed targeting Railway Undertakings and Infrastructure Managers business is a significant problem faced by the entire railway network (ENISA 2020). The implementation and integration of new technologies in the railway sector, such as the Internet of Things (IoT), Industrial Internet of Things (IIoT), automation, cloud computing, artificial intelligence (AI) et cetera, has introduced new types of risks in the railway operations and infrastructure. The Cybersecurity and Infrastructure Security Agency CISA (2021) pointed out that the fast adoption of high technology in Cyber-Physical systems has resulted in a complex scenario of interconnected systems and introduced new risks and threats to organizations cybersecurity and physical security functions that are not successfully converged.

The impacts of a cyber-attack targeting operational networks to damage physical infrastructure, or a physical attack aiming to get access to an organization's network and database system, can lead to unpredictable consequences. These types of attacks, also known as "converged attacks", can also happen simultaneously and increase the risks of casualties and damages in critical assets. To avoid such attacks, converged security risk management should be implemented (Aleem, Wakefield & Button 2013.). Yaacoub et al. (2020) add that the interconnected mesh of cyber-physical systems network environment is not developed with security by design in mind, leaving systems and infrastructures connected to it exposed to a wide range of vulnerabilities attackers can explore. Deka et al. (2018) emphasize that the detection, communication, and response methods utilized by physical and cyber security teams in railway operations, must have a well-integrated structure to deliver efficient information sharing. Additionally, a proactive early detection and response approach to better deal with the new emerging threat landscape targeting track-based transportation; and empower the systems, infrastructure, and processes, against potential attacks.

ASIS International (2005) defines security convergence as the capability of an enterprise to identify risks and their interconnectivity throughout the business operations and procedures and develop tailored solutions to solve this issue. Tyson (2007, 4) suggests that security convergence can be described as a jointed collaboration of security departments to achieve a common goal by using the available resources to improve cost-efficiency, threat identification, risk mitigation, and valuable assets protection.

Security convergence can be seen as cooperation between security teams that have been disconnected apart before and have found their way back to mutual collaboration. The benefits of converging cyber and physical security are, among others, the improvement in information sharing, reduction in double efforts to solve incidents, holistic alignment of both security divisions and leverage in the overall skills from both teams through cross-training practices, and more resilience and preparedness to deal with threats. (CISA 2021.)

This thesis aims to highlight the actions needed to assist Organization X and its members' operations in converging their security departments and enhancing its capabilities to detect, mitigate, and defend against converged threats targeting the railway network and infrastructure.

1.1 SAFETY4RAILS Project

The thesis topic was chosen in conjunction with our partner's (SAFETY4RAILS project) needs in the research, which is also aligned with the common goal of improving railway operations security and safety. SAFETY4RAILS (2020) is a two-year project funded by the EU, and the consortium has twenty-nine partners located in thirteen different nations. The project aims to

raise stakeholders' resilience against threats targeting railway infrastructures via cyber-physical joined attacks and provide approaches to increase customers' safety using intra-city metro and railway transportation.

SAFETY4RAILS project aims to develop an integrated and holistic approach to incidents prevention, detection, mitigation, response, and accidents recovery. The project has an innovative system implementation, the SAFETY4RAILS Information System, which is driven by Artificial Intelligence (AI) and will assist in the evaluation of strategies to be implemented as a preventive measure, and as a response to threat attacks (*SAFETY4RAILS* 2020).

SAFETY4RAILS goals, as shown in Figure1 below, are focused on outcomes englobing threat assessment to assist in identify and detect new risks targenting railway infrastructure, improving risk management and crisis forecast, strengthen resilience, promoting overall security improvements in railway network operations and familiarizing practitioners with SAFETY4RAILS information system.

Figure 1: SAFETY4RAILS goals (SAFETY4RAILS 2021)

1.2 Research Problem and Goal of the Study

The railway sector is facing a rapid digitalization and implementation of new technologies in its operations. Because most physical security systems use Internet Protocol (IP) based software, cyber and physical security teams can no longer be seen as two separated and siloed

departments. As one of the results of this fast-paced transition in railway operations, the security teams face well-structured hybrid or converged threats, targeting infrastructures, systems, and valuable information.

While the integration and implementation of ICT, IoT and other technologies in railway operations and services have been vastly studied by researchers, there is a lack of research related to assessing the measures needed to assist railway operators in identifying the needs for a successful security convergence. Railway operators need to develop procedures and guidelines to help determine the current requirements for integrated security teams and avoid gaps that could lead to incidents.

Identifying the needs Organization X and its members have for integrating cyber and physical security frameworks is vital to deliver maximum security and efficiency in response to threats that can cause disruption and causalities in their operations. As part of the SAFETY4RAILS project, this research highlights what additional information or guidelines Organization X needs to successfully collaborate in the convergence of the cyber and physical security environments in their associates' operations. The research will focus on Organization X's views, processes, and methods in its member's operations. Any other railway operators not associated with Organization X and the SAFETY4RAILS project are excluded from the scope of the thesis.

1.3 Research Question

The main question we were aiming to answer in our research was:

- What measures Organization X needs to enhance the integration of physical and cybersecurity environments in their members' railway operations and infrastructure?

There is a gap in the existing research on the guidelines needed to integrate physical and cybersecurity departments in railway operations and infrastructure. The answer to our research question would assist in proposing suggestions for the necessary actions Organization X's associates need to take in order to achieve a better integration in their physical and cybersecurity operations and infrastructure. Measures in the context of the research question imply guidelines or procedures needed by Organization X and its members to integrate physical security and cybersecurity frameworks.

1.4 Organization X

Organization X is an international association representing the railway sector and advocating for safer, modern, and dynamic rail network transportation. It was founded in the EU and is currently composed of 208 members in Europe, Asia, Africa, Oceania, the Middle East, and the Americas. The association members are encouraged to participate in the group meetings

and collaborate with ideas and suggestions to improve their operations and processes. The associates are often updated about new technological advancements, procedures for assessments, and supply chain and railway sector developments. (Organization X 2021.)

Organization X is one of the partners of the SAFETY4RAILS project. The mission of Organization X is to support railway transport in the development of a more sustainable and resilient environment. Also, enhance international cooperation and best approaches among associates; increase information sharing on railway operations and systems; and suggest innovative actions to promote cost-effective solutions. Organization X, as listed in figure 2, has established five action points in which it will be focusing on to act and serve its worldwide associates' operational needs (Organization X 2021):

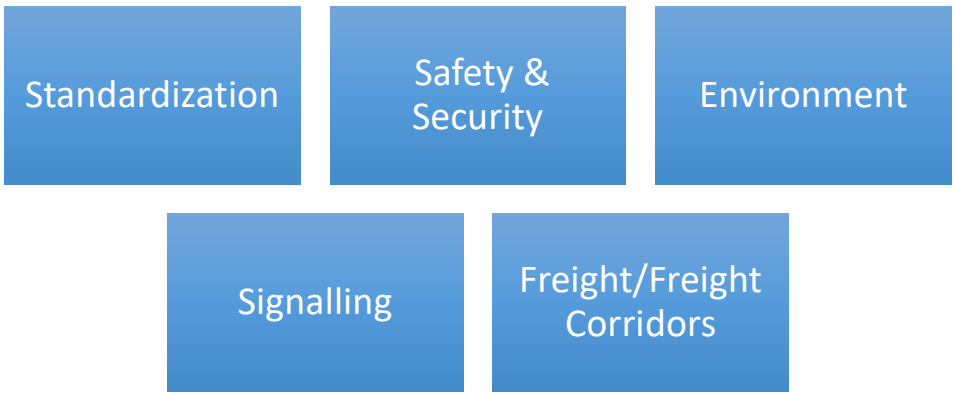

Figure 2: Organization X vital action points (Organization X 2021)

2 Theoretical Framework

A content literature review approach was used to review prior research and previously written articles about integrating physical and cybersecurity in railway operations to build the study's theoretical bases. The theoretical base focuses on exploring railway transport and its origins, understanding physical security and cybersecurity and their roles in railway transport. The literature review also looks at the current, and emerging security threats to mass transit operations and the measures rail and metro operators need to integrate their physical and cybersecurity frameworks. The main themes explored in the knowledge base include the need for and benefits of integrating physical and cybersecurity in mass transit operations, guidelines, and procedures best suited to incorporate physical and cybersecurity of rail and metro environment. This section contains the literature review we conducted in assessing the guidelines or requirements railway operations need for the convergence of physical and cybersecurity of railway and metro operations.

2.1 Railway Transport Background

According to Bagwell, P., & Bagwell, P (2006), many of the technologies invented during the industrial revolution, such as the invention of the steam engines, their adaptations to mechanical traction, and the creation of specialized tracks, made it possible to create the modern railway system. Bagwell et al. (2006) define contemporary railway transport "as a publicly controlled means of transport possessing the four distinctive features of a specialized track, mechanical traction, accommodation of public traffic, and passengers' conveyance". While the Economic Times (2021) sometimes describes rail transport as a transport method in which wheeled vehicles (carriages) are pulled by a train driven on and guided by tracks (railroads) to transport goods and people from one place to another. Since the invention of the railroad in the early 19th century, in many countries worldwide, especially in European countries, the railway system has played a significant role in their economic expansion by revolutionizing how people travel, and goods are transported to long and short distance destinations.

According to Encyclopedia Britannica (2019), the first fully operational passenger and cargo-carrying rail transport with a steam-powered locomotive engine was launched in Britain by Stockton & Darlington Railway company in 1825 during the latter stages of the Industrial Revolution. In the subsequent years, railway transport has gone through many modernizing phases, be it new railway technologies coming online or how rail transport fits into a country's transport infrastructure. These modernizations included, among other things, the invention and transition to electric locomotive trains between the mid-19th century to the earlier 20th century, the conception of the underground or Metro railway system to meet the increasing needs of urbanization in major cities. Bellis (2020) adds that creating a high-speed intercity railway system and adapting ICT components to the railway transport system are among the latest modernization in railways.

Rail transport is generally divided into freight and passenger rail transport, including metro or mass transit transport operations. Historically the railway sector has been governed by rules surrounding interoperability, safety, dangerous goods management, and certification at the international, European, and national levels. (ENISA 2020).

ENISA (2020) lists the leading players in the railway transport sector as:

- The railway undertakers are responsible for providing passenger and freight rail transport services to customers and the public.
- The infrastructure managers are tasked with establishing, managing, and maintaining rail infrastructures such as train power supply, station operations, signalling, and traffic management.

According to the EU (2008) publication, *TOWARDS AN INTEGRATED EUROPEAN RAILWAY AREA*, railways constitute a shrinking share of the land transport sector in many developed countries, including European countries. For the last few decades stretching to the late 1960s, railway transport for both goods and passengers has declined while road transport, particularly goods transported on the road, has tripled in the same period. The publication also highlights that railways have struggled in freight and passenger transport: for example, rail's share in passenger land transport in the EU in 1970 was over 10%, but by 2006, it had plummeted to stabilize at 6.9%. In absolute terms, however, there was more train travel. (EU 2008.)

A study conducted by Arvis, Saslavsky, Ojala, Shepherd, Busch, & Raj (2014) has underscored the importance of the transport sector in a country's critical infrastructure. Also, how physical connectivity in the urban and rural areas help the socio-economic development of a nation and increase its economic-wide productivity. In the EU, rail transport had an estimated turnover of EUR 60 billion in 2004 and generated EUR 34 billion added value to the economy, accounting for roughly 900 000 jobs (EU 2008).

The US homeland security department (DHS) lists transportation and its sub-sector of rail transport, including passenger and freight rail, as one of the crucial components compromising the US's critical infrastructure sectors (CISA 2021). Critical infrastructure refers to physical and cyber systems and assets essential to any country's socio-economic development. Their failure or destruction would have a crippling effect on the nation's physical security and public health and safety (DHS 2021).

These days, the widespread consensus supported by researchers like Logan, Nelson, McLellan & Hasting (2020) is that railways are more environmentally friendly and cause less pollution to the environment than road and air transport. For example, Logan et al. (2020) describe how "Conventional train emissions are 2.6 times lower than conventional fossil fuel cars". This widespread perception is closely related to the primary energy source for each mode, namely electric power for most modern trains and fossil fuel for most air and road transport. As a result, the EU has ear-marked rail transport as an integral part of its development and Green Deal initiative, which aims to assist clean, affordable, and healthy private and public transportation and achieve a 90% reduction in transport emissions by 2050 (EU 2008). The Economic Times (2021) writes that many consider rail transport one of the most dependable forms of transport from a safety perspective. Compared with other forms of transportation, railways are generally least affected by weather changes and turbulences, such as rain or fog.

2.2 Physical Security in Rail Transport Environment

Physical security can be described as using resources to safeguard individuals' well-being and protect their physical and intellectual properties from threats such as theft, destruction, and exploitation (Contos 2007). On the other hand, Cobb (2021) defines Physical security as "the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution". The idea of people protecting themselves and their belongings from some perceived threats has existed for many thousands of years. The walls of the excavated Jericho city in Palestine, which is considered one of the earliest human settlements dating back more than 4000 BC, show some form of physical security being implemented at the time (GRAVES 2006). Designing physical security must be layered as no one physical security solution can meet an organization's all security demands. USDA (2021) recommends that "Protection of assets must be based on a realistic assessment of the risks associated with the criminal and terrorist threats likely to be directed at the assets in their actual locations". Or in other words, the risk-based methodology must be used in designing an organization's physical security posture.

According to Cobb (2021), a successful physical security program relies on how an organization implements and maintains the three most important layers of a physical security plan, which are access control, surveillance, and testing:

- Access control refers to the steps taken to limit the exposure of certain assets to authorized persons only. ID badges, keypads, and security guards are typical examples of access control mechanisms. These barriers, however, might vary considerably in terms of technique, approach, and expense. (Cobb 2021).
- Surveillance covers anything from patrol guards, burglar alarms, and CCTV to sound and movement sensors that keep track of who goes where and is an essential physical security component for preventing incidents and their forensic analyses. (Swinhoe 2021).
- Because physical security is a preventive and incident response tool, companies must regularly test their security policies and procedures. Fire drills, for example, are an essential exercise for schools and buildings since they aid in the coordination of big groups and their reaction technique. When it comes to organizational unity, testing is becoming increasingly important (Cobb 2021).

Graves (2006) writes that Since the 9/11/2001 terrorist attacks in New York, there has been a renewed emphasis on physical security, resulting in governments, businesses, and industries allocating sizable resources to improve their security posture. The author argues it is a testimony to the new emphasis on physical security that transportation security is being revamped

for passenger and cargo protection; terminal and port security are also being upgraded. Additionally, this new emphasis on security has resulted in US local governments spending more than $70 million per week on security.

The nature of rail and metro operations and their crucial role in a country's critical infrastructure makes maintaining their safety and security a priority. According to UIC (2021), physical security systems in the railway and metro environments include:

- Access control systems such as station turnstiles to manage and control passenger flow in and out of stations.
- Perimeter protection and sensor barriers prevent vandals and inattentive passers-by from intruding on unauthorized or sensitive parts of the rail and metro infrastructure.
- Surveillance systems such as video analytics surveillance cameras are installed through the network to monitor, record, and alert any threats to the day-to-day safety and security of rail and metro users and employees.
- Fire detection and extinction systems and tunnel movement detection systems are also integral in the rail and metro physical security framework.

Physical security elements in railways such as video surveillance, access control, and intrusion detection systems are becoming increasingly database-driven and network-delivered. In other words, IT (Information Technology) and physical security are increasingly intertwined, thus creating the need for an integrated approach to railway security.

2.3 Cybersecurity in Rail Transport Environment

Cybersecurity is a set of rules, mechanisms, and technical programs implemented to protect and prevent information technology infrastructure from misuse, cyber-attacks, and unauthorized access (De Groot 2020). On the other hand, Shea, Gillis, and Clark (2021) characterize cybersecurity as "the protection of internet-connected systems such as hardware, software and data from cyber threats". Practice individuals and businesses utilize to prevent illegal access to data centres and other communications devices. As both definitions make clear, cybersecurity focuses on protecting digital information and systems from possible threats. In contrast, Information security, which is sometimes confused with cybersecurity, is broader and deals with protecting both digital and physical data.

According to Mutune (2021), computer security concerns were easily recognizable throughout the 1970s and 1980s. Most of the threats came from malevolent insiders who wanted to view documents they had no access to. At the same time, computer security in software programs and risk and compliance governance emerged independently. Network breaches and viruses

existed throughout the 1970s and 1980s, but they were primarily utilized for reasons other than financial gains.

Many researchers trace back the first computer worm to a graduate student at Cornwell University named Robert T. Morris, who was interested in the scope and scale of the internet and in 1988 built a worm to test it. A programming mistake allowed the worm to infect machine after machine, clogging networks. The Morris worm has prompted other people to investigate how they could build deadlier and more powerful worms and viruses. Worms and viruses, in turn, started the development of antivirus software to combat worm and virus attacks, which marked the beginning of a whole new sector in computer security. (Mutune 2021.)

Because governments and companies collect, process, and store a large amount of personal and sensitive information such as financial and medical records on computer networks, cybersecurity plays a unique and vital role in our increasingly interconnected society (De Groot 2020). Shea et al. (2021) argue that cybersecurity can help protect against various cyber threats such as social engineering, phishing, malware, and ransomware. Hackers can use these methods to gain unauthorized access into an organization's systems and steal sensitive information such as credit cards or login credentials.

There are six commonly agreed cybersecurity features: application security, information security, network security, disaster recovery planning, operational security, and end-user education (Shea et al., 2021). According to Chai (2021), the most well-known data storing model organizations are using is the CIA (confidentiality, integrity, and availability) triad, or sometimes referred to as AIC (Availability, Integrity, and Confidentiality) triad. It is a paradigm meant to govern rules for information security inside an organization. The significance of the CIA triad security model is self-evident, with each letter reflecting a fundamental concept in cybersecurity.

Since the 1990s, due in part to the internet, digitalization has been accelerating throughout all economic sectors, government agencies, and society at large, and railroads are no exception. Scordamaglia (2019) writes that firms in the rail transport sector have adopted a wide range of new digital services and apps, whether for delivering more information and leisure services on board trains, enhancing asset maintenance, and monitoring additional automated operations. The author adds that many stakeholders see the changes caused by digitization in rail transport as both an opportunity and a problem, given the benefits and threats that accompany them. Indeed, digitalization will require a shift in thinking and business structures. Rail digitization will also necessitate financial investment and a cybersecurity plan; addressing these issues would allow digitalization to increase the railway sector's efficiency and competitiveness (Scordamaglia 2019).

As indicated in Figure 3, Monteagudo (2021) highlights some of the characteristics of rail infrastructure that can make them attractive targets for cyber-attacks, and they include:

- The increasing number of connected transportation systems on trains.
- Rail infrastructure is distributed across vast spaces.
- Supply chain and technology variations.
- Long equipment lifespans and certification processes.
- Once a system component is certified, it may become outdated, particularly in cybersecurity, given the rapidly developing threat landscape.
- There is a high level of integration between the rail sector's information technology (IT) and operational technology (OT) frameworks.
- Historically, the rail industry has been highly safety-oriented, and it is finding it challenging to integrate the two worlds of cybersecurity and safety.

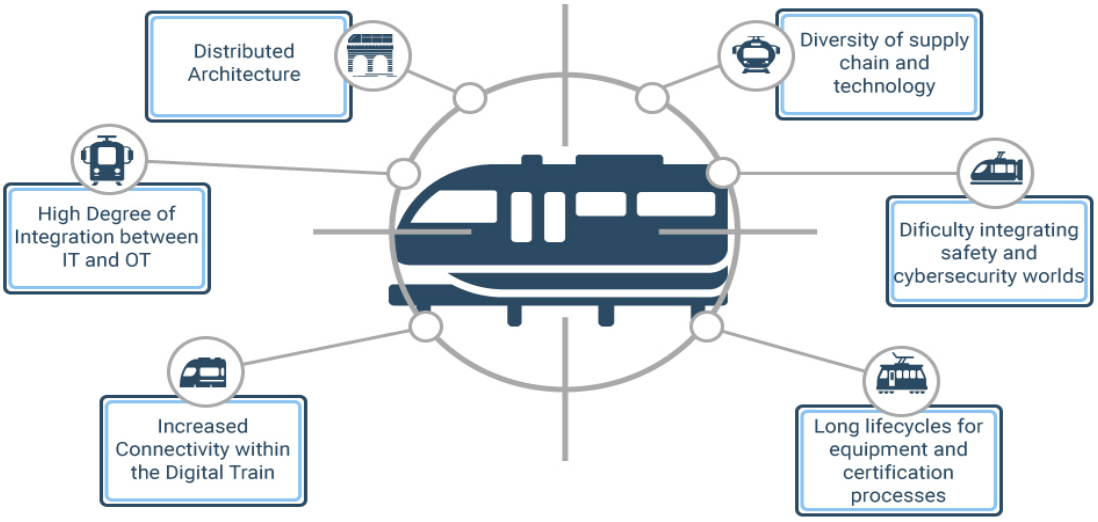

Figure 3: Key challenges to secure the railway infrastructure (Monteagudo 2021)

Digitizing the railways and integrating ICT components into the Train Control and Monitoring System (TCMS) has helped lower operational costs for rail operators and improved end-user services. On the other hand, it exposed the system to cyber-threats, thus increasing cybersecurity's significance for railway systems' overall security framework (Rekik & Berbineau 2018.).

According to ENISA (2021), the challenges rail operators face in implementing adequate cybersecurity include issues with the digital transformation of the core business of metro and

railway operations, such as the introduction and adaptation of IoT into the rail and metro environment and low cybersecurity knowledge and awareness among staff. Although, cybersecurity awareness is improving partly due to the increasing threats and attacks originating from the cyber domain.

Other challenges listed in the report include, among others, the distribution of rail and metro infrastructure over a vast territory of land and the existence of some legacy systems in their operations. Also, because safety is a paramount requirement in the mass transit sector, the lack of convergence of cybersecurity with the overall safety frame of rail and metro operations is another issue that hampers proper cybersecurity in railway environments. (ENISA 2021).

2.4 Existing and Emerging Threats to Rail Transport Security

Terrorism, sabotage, and vandalism are significant physical threats facing railway systems. Terrorism remains the most significant threat, and between the years 2000 and 2004, terrorists have attacked railway systems around the world, 27 times more than air transport. Railways remain an attractive target for terrorist attacks due to the possible mass casualties' attacks can cause and the panic it can ensue in the general population. Most research into railway systems' security has shown that the railway network's security challenges are related to the network's hallmark of being open and accessible while covering a large geographical area. (Flammini 2012.)

According to Riley (2004), terrorists are likely to see psychological gains from striking passenger transit networks. Rail transit, like air travel, requires passengers to be willing to entrust their safety to others. An attack on railways is likely to make people, at least momentarily, hesitant to go on the passenger rail system. Ridership would most likely decline due to the resulting security measures causing higher charges or longer travel times.

Passenger trains are unlikely to achieve a high level of security in the same way that airports and airplanes have accomplished. Because passenger profiling, screening, metal detectors, X-ray machines, explosives sniffers, hand searchers, and armed guards are used extensively at airports. These methods are difficult to implement in the rail environment. Also, physical space limitations in some areas and high commuter concentrations make it almost impossible to build rail station "safe zones" like those found between check-in desks and departure gates at airports. (Riley 2004.)

Michael Jenkins and Butterworth (2020) analyses of Mineta Transportation Institute's (MTI) database of attacks on public surface transportation since 1970 has found that terrorist attacks against passenger rail transit are statistically uncommon in the developed world, with about seven attacks per year against all economically advanced countries combined. However, the

authors add that unearthed schemes and attempts show how terrorists are still interested in striking transportation targets. The vast majority of terrorist attacks against passenger rail transit are meant to disrupt travel or cause casualties. Most of the attacks, 87% and most of the casualties, stem from attacks on passengers on trains and stations, i.e., where people assemble and are present.

Some of the most well-publicized terrorist attacks on rail and metro environments include the Madrid commuter train attacks on March 11, 2004; the London attacks on July 7, 2005 (three of which occurred on the Underground network); the Moscow Metro suicide bombings in 2010, and the March 22, 2016, suicide attack on Brussels' Maelbeek subway station. All these attacks resulted in death, injury, and disruption. These are highly unusual phenomena, yet they can significantly influence public perception about rail and metro security (Reuters 2017).

Historically the main threats facing rail and metro operations, such as terror attacks, were from the physical sphere. In the meantime, threats originating from the cyber domain, such as hacking, distributed denial-of-service (DDoS) and ransomware, are increasingly becoming a significant concern for the rail sector. They could be used to cause mayhem on the system on their own or as a complementary means of attack with physical attacks. (Chen, Schmittner, Ma & Dong 2015.)

The November 2016 cyber-attack on San Francisco Municipal Transport Agency was one of the most prominent examples of how cyber-attacks are affecting the rail transportation industry. Nearly 2,000 computers were malware-infected with HDDCryptor malware, allowing public access to the Agency's network. Although, the Agency's capacity to provide transportation via its fleet of light rail vehicles, streetcars, trolleybuses, and hybrid buses was not jeopardized. Its network was compromised, and ticket machines, payment services, and emails were all impacted. The hackers' demands of a ransom in bitcoin payments equivalent to $ 102 000 was rejected by the San Francisco municipality, and the Transport Agency was able to restore the system. (Pearce 2021.)

2.5 The Need for and Benefits of Converging Physical Security with Cybersecurity

These days, very few organizations rely entirely on one set of security mechanisms to protect and safeguard their assets. Most firms use security systems that implement a combination of physical and cybersecurity procedures. However, one must understand the functions of each other's security frameworks to deploy physical security and cybersecurity measures side by side appropriately.

Organizations willing to invest in and incorporate IoT networks into their operations present new threat possibilities and new risks. For example, IoT technology has enabled more powerful physical security systems than ever before, including IP security cameras and real-time

video analytics systems. Still, the network-connected hardware that powers them provides a unique entry point for bad actors seeking to acquire sensitive data or even jeopardize physical security. IoT networks must maximize advantages and minimize possible hazards by being aware of the developing connections between cybersecurity and physical security (D'mello, 2019).

The Integration of control systems and digital communication components, such as GPS tracking devices, smart controllers, and real-time monitoring into railway services and operations, brought many benefits to operators and the public. It has also aroused concerns about the consequences that targeted attacks on such systems in railway infrastructure could cause. A well-integrated approach between physical and cybersecurity frameworks in railway operations is needed to provide a secure and efficient service to its customers (Deka & Mashrur 2018). The consequences of a cyber-attack targeting railway operations network to damage physical infrastructures or vice versa could result in many casualties, mobility disruptions and substantial monetary loss.

Lalond (2018) writes that teams in separate departments deal with most organizations' cybersecurity and physical security responsibilities. Usually, their only interaction occurs when responding or investigating a security incident. Security incidents can occur due to this lack of information sharing between siloed teams. It can result in an organization having a partial response and not seeing the entire picture from a response perspective, a mitigation perspective, or even a deterrence angle. The author contends that organizations can detect and respond effectively to many security threats by merging physical and cybersecurity infrastructure. Carlson et al. (2021) also argue that an integrated approach to physical and cybersecurity is needed to meet modern railway operations' security challenges.

Physical security and cybersecurity convergence can be described as a formalized cooperation between previously fragmented security teams and tasks. In this case, cooperation refers to a concentrated, results-oriented attempt to work together. This type of cooperation involves defined procedures and the assumption of responsibility, rather than a concept that emphasizes form above function, which causes much of the existing resistance against security convergence. Although merging organizational charts is a highly reasonable approach to promote responsibility and collaboration, many companies may have good reasons for not doing so. (Slater, 2005.)

According to the ASIS (2019) security report on the state of security convergence in the United States, Europe, and India, 36 percent of firms that integrated physical and cybersecurity identified difficulties with personnel skillsets and working cultures as the primary obstacle to convergence. At the same time, 24 percent of businesses who have integrated their security have identified turf attitude and segregated teams as significant challenges to security

convergence. On the other hand, over one-fifth of all respondents, 22%, said they had no problems combining departments.

The ASIS (2019) study on the state of security convergence was launched to provide appropriate benchmarks for comparing strategies, plans, and operations and determine best practices for developing more successful and cost-effective security and risk operations. Table 1 below highlights the main benefits of converging physical and cybersecurity, such as improved security alignment with business goals, cost-effective security structure, improved information sharing, and an organization better equipped against potential threats.

Better Business goals and security alignment	Cybersecurity and physical security have traditionally been viewed as independent from the broader business strategy. However, a converged threat landscape means that physical security and cybersecurity threats must be understood and treated as business risks.
An efficient security framework	Organizations can save time and money spent on managing segregated teams and bridging communication gaps. Organizations can also save staffing costs by eliminating redundant security responsibilities.
Improved communication & knowledge sharing	Because of a more integrated security strategy, employees who were previously split by turf allegiance can now share information and work together as a team. Also, cross-training due to integrated physical and cybersecurity makes employees more versatile and aware of areas that were not previously part of their job descriptions.
A more secure enterprise	Incorporating physical and cybersecurity environments improves firms' awareness of security threats, especially when they overlap. With integrated physical and cybersecurity, organizations are better equipped to anticipate dangers and deal with them before they become a significant problem.

Table 1: Benefits of converging physical security and cybersecurity (ASIS 2019)

CISA (2021) states that physical and cyber assets from energy and transportation to agriculture and healthcare are increasingly connected due to technological advances. Thus, an integrated threat management approach to cyber and physical security reflects an in-depth awareness of the rippling effects of many organizations' increasingly linked cyber-physical infrastructures. Also, CISA (2021) insists that "the benefits of converged security functions outweigh the challenges of organizational change efforts and enable a flexible, sustainable strategy anchored by shared security practices and goals.".

3 Methodology

In this chapter, we described the steps followed to design our research, the information gathering method used to find answers to our research question, and the content analyses applied. We adopted an exploratory research design to structure the study, a qualitative data collection method, including a literature review, a semi-structured qualitative interview, and a content analysis approach to exam the data. This methodology's flow structure was chosen because it presented the best research approaches to obtain valuable insights related to Organization X's members' current needs for better integration of their cyber and physical security frameworks.

According to Kothari (2004), a qualitative approach focuses on understanding patterns and attitudes where the research's central point is the quality or type of phenomena studied. Adams, Khan & Raeside (2013) point out that qualitative research aims to provide a detailed understanding of the experiences, needs and problems experienced by the person(s) or object(s) investigated.

Dudovskiy (2021) explains that exploratory research design is applied in studies where the research problem has not been adequately examined or no previous study has been carried out. Also, exploratory research design does not provide an irrefutable answer to a research question. Still, instead, the research results identify different elements and possibilities to solve a problem and answer the research question, producing qualitative information. Swedberg (2020) argues that exploratory research assists in building empirical theories or hypotheses while researching a new phenomenon or idea.

The research design implemented in the thesis followed a logical flow to understand better the phenomenon studied, gather valuable data and inputs, analyze the outcomes, and provide the best answer to our research question. Figure 4 below presents the research design structure and sequence of the study in the thesis and the key points we focused on each phase of the design process, starting from research problem regarding the convergence of physical security and cybersecurity in railways to the recommendations and conclusions we reached:

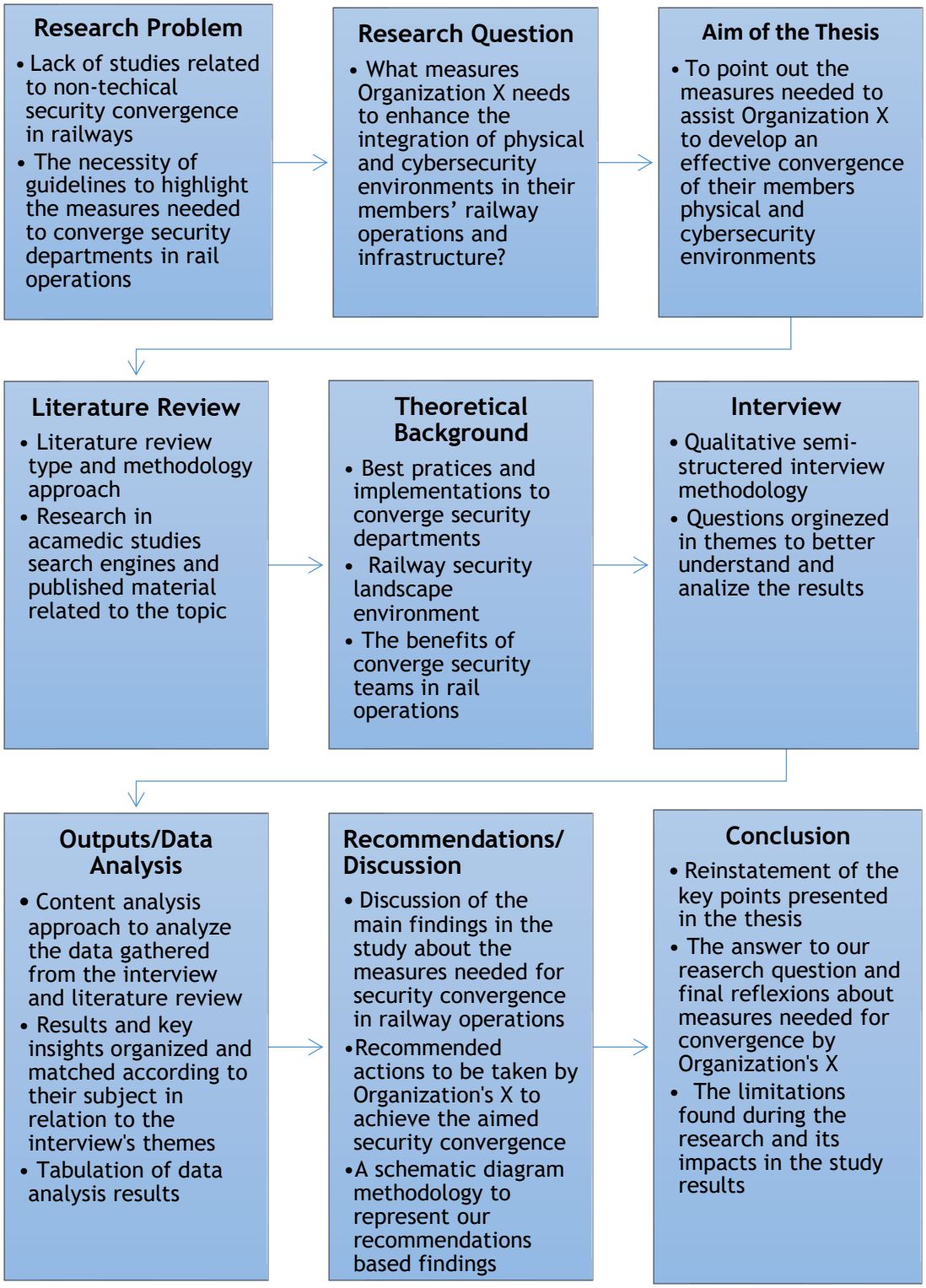

Figure 4: Research design process structure implemented in the thesis

3.1 Case Study Approach

The qualitative data collection approach implemented in our research was a case study method. According to Gillham (2000), a case study is a research method that aims to answer specific questions by extracting and examining a variety of evidence in the case environment. Based on the data collected, build the best answer to the research question. Yin (2003) points out that a case study is a factual research method that assists in providing outputs to a specific inquiry, where there is no comprehensive understanding of a particular case and its circumstances. Baxter and Jack (2008) add that qualitative case studies assist in exploring a particular event through a multitude of optics, permitting the researchers to understand the multiple aspects that characterize and results in the studied phenomenon.

According to Dudovskiy (2021), case studies are a well-known research method implemented in businesses and organizations. Its primary purpose is to analyze a particular and current issue experienced by organizations or individuals within a specific environment's borders. An exploratory case study aims to answer the research questions of "what" or "who" in the phenomenon studied, and often interviews or questionnaires supplement the data collection.

The advantage of using a case study research method includes the possibility of studying the phenomenon in real-life situations and environments, flexibility in merging qualitative and quantitative data analysis, and the chance of capturing more complex results. As for disadvantages, the absence of accuracy in the results, difficulty finding grounds to generalize conclusions and challenges in analyzing the data collected can be mentioned. (Dudovskiy 2021.)

We chose this method for our thesis because we believed that a qualitative case study approach provided the best framework to answer our research question; as we could explore the specific needs for security convergence based on Organization X's perspectives; it would give us a deeper understanding of the critical points that are necessary to develop guidelines for efficient integration of the security environments from Organization X' members, and provide the outcomes to answer our research question. Also, we could not find any previous studies related to a non-technical convergence of physical and cybersecurity specific to the railway sector, which led us to implement a case study approach to gain more detailed insights about the topic.

3.2 Semi-structured Interview

There are three types of interviews that can be used in qualitative studies: structured, semi-structured, and unstructured interviews. A structured interview is a type of interview where the structure style is not so flexible and usually follow strict rules as a guide for the interviewer. This stricter interview-style aims to only gather the answers without exploring further

insights that the interviewee might mention. Semi-structured interviews also have a pre-determined guiding structure but more flexibility to gather additional insights and explore other new topics that the interviewee might bring up while answering the questions. Also, this type of interview allows the interviewer to get more insights into the participant ideas, opinions, and expectations. Unstructured interviews are very flexible and do not follow any type of pre-determined questions or framework, and often many interviews are usually required to gather all the information needed. (Statics Solution 2021.)

A qualitative semi-structured interview was the data collection method chosen to gather information and insights about the actions needed to better integrate physical and cyber security departments from Organization X's associates. Gillham (2000) emphasizes that a semi-structured interview is one of the most effective ways to gather information in an interview when used in a case study due to its structural flexibility and deceptive simplicity. Although interviews can be very time-consuming, they usually provide critical elements to help researchers understand the analyzed phenomena.

To better understand the needs and necessary guidelines to integrate the physical and cybersecurity departments in this case study, a semi-structured interview with open-ended questions with a key Organization X stakeholder was used to obtain the primary research source. The interview consisted of 15 questions (Appendix 1) grouped into themes, as shown in Figure 5, ranging from current implementations, challenges for implementing convergence, resources, skills, and knowledge required to integrate physical and cybersecurity to security policies, standards, and management commitments.

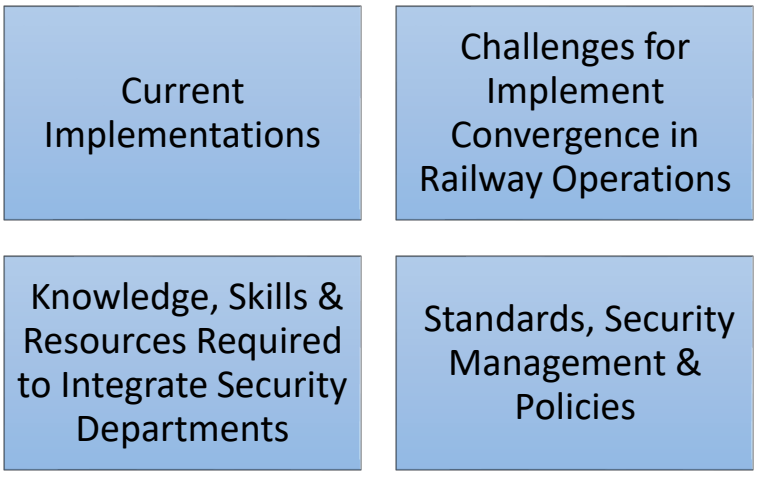

Figure 5: Interview themes structure

During the interview, we took notes to ensure that opinions, comments, and ideas collaborated to find the research answer. If necessary, we could send a summary of what we took to the interviewee to ensure that the insights were adequately understood.

3.3 Literature Review

A literature review type was conducted as a secondary research source to establish the correlation between the references and the theoretical framework in the research, such as academic journals, peer-reviewed articles, magazines, and books related to the topic. According to Grant & Booth (2019), a literature review aims to assist the researcher in finding previously published studies related to the topic searched and point out similarities, differences, exclusions, or gaps, that can be associated with the explored subject.

We chose literature related to our thesis topic for review, using keywords to search the study topic in academic search engines such as Google Scholar, Laurea Finna, ProQuest, Science Direct, Springer Link, Research Gate, Elsevier, and others. The keywords used in the academic search engines vary from railway security convergence, converging security in rail, railway security integration, cybersecurity in railway, physical security in railway, et cetera. We could not find many studies and articles specific to the convergence of physical and cyber security in railways, nor studies on convergence needs. Most of the studies that covered the topic were from a technical point of view, not at the operational level. We then widen our field of research to look at the convergence of physical and cyber security from a general enterprise perspective that could be adapted, integrated and applied in railway operations.

3.4 Content Analyses Approach

To analyze the qualitative data collected, we adopted a content analysis approach. Content analysis is a method to exam the data gathered in semi-structured interviews and a concise way to present the findings. The results from the interviews would then be categorized, coded according to their context, and then tabulated. Tabulation is a common and practical way to represent the results found in a content-analysis process. (Adam et al. 2013, 161-163.)

Based on the nature of our thesis, we have chosen to implement the tabulation content analyses approach, as it is more suitable to represent the critical points obtained from our qualitative semi-structured interview. Organized by their context, the main insights gathered from the interviewee were associated with one of the interview's theme categories, then tabulated to present the several factors that should be considered in the assessment of Organization X's security convergence needs. This information provided us with an overview of the current actions that Organization's X has taken to assist in the physical and cybersecurity convergence process; the challenges involved in this implementation; the resources and skills needed; the necessary commitment by decision-makers; and the policies and standards required for successful integration. The literature review's main insights were also added in the mentioned interview's theme categories and tabulated to provide additional insights related to current methods and best practices applied in other sectors that could benefit this integration process in the railway environment.

After the content analysis was completed, the assembled information was taken into consideration to propose the recommendations to develop the necessary measures to support Organization X's members in achieving a better integration in their physical and cybersecurity operations and infrastructure. Also, to collaborate with the SAFETY4RAILS project in improving the safety and security in railways.

3.5 Reliability and Ethical Considerations

As mentioned by Bryman and Bell (2007), some essential principles that should be followed in ethical considerations are:

- Full consent should be obtained from the participants before the study.
- The protection of the privacy of research participants must be ensured.
- An adequate level of confidentiality of the research data should be provided.
- The anonymity of individuals and organizations participating in the research must be guaranteed.
- Any deception or exaggeration about the aims and objectives of the study must be avoided.
- Any misleading information and representation of primary data findings in a biased way must be avoided.

Considering these aspects while carrying out our research with Organization X, the ethical considerations applied were:

- The interviewee in the research was fully informed about the implications of participating in such and how the information will be used and processed.
- Assurances of privacy and anonymity from the respondent and the organizations involved in the study were provided.
- Commitments to follow the laws and regulations were made to Organization X, the SAFETY4RAILS project and a contract was signed with our educational organization.
- All necessary steps were taken to avoid plagiarism and maintain the highest level of objectivity and analysis throughout the research.

4 Research Findings

This chapter shows the research findings from our interview with a high-ranking representative of Organization X and the literature review we conducted into the phenomena. The results collaborated to help us answer our research question about the measures Organization X needs to enhance the integration of physical and cybersecurity environments in their

members' railway operations and infrastructure. As seen in Table 2 below, this chapter followed the same pattern as our interview, and points out the areas in need of guidelines for security convergence by highlighting the current level of physical and cybersecurity convergence in the operations of Organization X and its members, the hurdles they may encounter in merging security departments, the resources and skills required for an effective security integration, and the role security standards and policies in the railway sector play in ensuring an efficient integration of physical security and cybersecurity.

Current Security Implementation	• In most railway organizations, physical security is usually the responsibility of the corporate security department. At the same time, the IT department is responsible for dealing with cybersecurity issues. • Railway operators increasingly view an integrated security framework as an essential and overdue step in dealing with the ever-changing and more hybrid security threats challenging the current railway security structure. • Although Organization X shares information related to physical security implementations and training to its members through their internal communication channels, procedures dedicated to physical and cybersecurity convergence has not yet been formulated.
Challenges to the Security Convergence	• Current railway security structure of Siloed and different departments dealing with physical security and cybersecurity separately increase security vulnerability. • There is a lack of and an increasing need for railway specific cybersecurity experts to deal with the challenges raised by adapting ICT systems like IP connected signalling to the railway infrastructure. • Human factor issues such as security awareness can be obstacles in converging physical and cybersecurity.

Resources, Skills, and Knowledge Needed for Security Convergence	• The establishment of seamless communication channels for information sharing and clear guidelines for convergence. • The need for incorporating artificial intelligence into the organization's security infrastructure. • To close the skills gap, staff cross-training to learn about the operations and procedures in both physical and cybersecurity environments.
Standards, Security Management and Policies.	• EU member states are reluctant to accept any EU-wide regulation because national states regulate railways. • Rail-oriented cybersecurity standard is under development as part of an EU sponsored sideway project but nothing specific for physical and cybersecurity convergence. • The current security standards are insufficient to provide guidelines for converging railway physical security and cybersecurity.

Table 2: Research Findings

5 Discussions

In this chapter, we discuss the significance and applicability of our findings. It focuses on describing and assessing what was discovered about security integration and how it pertains to our literature review and research aim of highlighting the measures Organization X and its members need in converging their physical security and cybersecurity departments.

5.1 Current Security Implementations by Organization X's Members

Our literature review on convergence has shown that the security structure of separate departments handling physical security and cybersecurity exists in the railway sector and is common to other enterprises in the corporate world. Lalonde (2018) points out that the security department handles physical security in most organizations, whose staff typically come from a law enforcement background. In some cases, physical security is outsourced to the

site-owners of the building the company operates in. Additionally, the writer adds that the IT department manages cybersecurity in most enterprises.

We discovered during our study that organizations are increasingly becoming more aware and are recognizing the need for a more holistic approach to security. This awareness is due to new security threats and vulnerabilities developed due to the advent of modern technologies with Internet Protocol (IP) networks, including building systems, security applications, and video monitoring. To this end, projects like SAFETY4RAILS, which this study is part of, focus on assessing railway organizations' needs in terms of information and guidance in integrating physical security and cybersecurity departments.

5.2 Challenges to the Convergence of Physical and Cybersecurity

Many experts point out that the most significant impediment to convergence is the disparity in culture and skillsets between physical and cybersecurity departments. CISA (2021) points out that the departments responsible for physical security and cybersecurity are still viewed as distinct. Also, it argues that when security experts work in silos, they do not have a complete picture of their company's security threats. Lalonde (2018), on the other hand, mentions that some experts argue that physical and cybersecurity departments have divergent cultures. Therefore, it is preferable to keep them separate because salary, management, job security, and budget concerns can impede integrating functions or departments.

One may conclude that physical and cybersecurity convergence does not automatically mean converging two distinct departments. But it is instead consolidating and harmonizing the overall security policies, technologies and functions of the organization and overcoming what some experts classify as turf and silo operating culture of non-converged organizations. Designing and implementing a clear, holistic security strategy is vital for physical and cybersecurity convergence. In our view, to achieve these goals and overcome the challenges mentioned above, strong senior management support and buy-in is required.

5.3 Knowledge, Skills, and Resources Needed for Physical and Cybersecurity Integration

The need for cross-training between physical and cybersecurity employees is a theme we picked up from our literature review. For example, both Slater (2005) and Lalonde (2018) point out that cross-training can help both departments' employees better grasp the other's position and how their objectives and tactics fit into the overall security strategy. Also, the writers add that such training is essential to educate staff on the advantages of convergence and how it may assist, enhance operations, and protect against threats. It is reasonable to

assume that cybersecurity experts are unlikely to know how to prevent an authorized entry into a company property, just as physical security guards are unlikely to understand how to act during a cyber-attack. Thus, cross-training from our perspective is a critical component of achieving a smooth convergence of physical security with cybersecurity. Additionally, there is a need for broad guidelines to address security convergence challenges such as structural and culture differences, personnel skills gaps, technological best practices and business goals, and security strategies divergence.

5.4 Standards, Security Management and Policies

Our literature review showed that different organizations might opt for different approaches to converging physical security and cybersecurity due to organizational culture and size; however, developing a holistic security strategy is still necessary for security convergence.

According to Lalonde (2018), convergence's goal is not merely to merge two security departments into one. The objective is to create highly effective security policies, accountability, and governance that integrate the efforts of both departments to ensure that they are prepared to collaborate to prevent threats and provide the organization with a consistent, comprehensive view of its physical and cyber security. In other words, there is no one-size-fits-all approach to the convergence of physical and cybersecurity. Also, the objective is not just merging two departments for budgetary or other considerations instead. The aim is to establish security rules, governance and accountability that integrate the operations of both physical security and cybersecurity personnel to ensure that they are ready to work together to avoid and manage risks.

6 Recommendations

Based on the content analysis results from the interview with the key stakeholder from Organization X's security management team and the main insights gathered from the literature review, we elaborated recommendations to assist Organization X's members in converging the physical and cybersecurity departments in their railway operations. Because the flawless integration of three factors, People, Process and Technology, is required for security convergence, our recommendations are grouped in these intertwined pillars. In the People section, we highlighted the actions that should be taken to improve employee and employers' knowledge and skills to assist in implementing and maintaining converged security. In the Process section, we recommended the actions Organization X's and its members should take to implement policy and governance framework for effective security integration. Finally, the Technology section highlights the technological best practice required from a security

governance perspective. In the diagram shown in Figure 6 below, we point out the recommended guidelines we believe Organization X and its members should consider while designing and implementing a convergence action plan in their physical and cybersecurity departments:

People	Process	Technology
• Analyse existing physical and cyber security personnel' skill sets to discover possible skill gaps and overlapping tasks within departments, also develop strategies for upskilling people to operate within a unified security team. • Create a cross-training program with an educational convergence knowledge base and a thorough understanding of each other's tasks and responsibilities, as well as how integrating both environments will benefit Organization X's members in achieving a high level of safety and security in its operations. • To determine the best method for convergence, Examine the organization's culture and security teams before executing a convergence strategy. Assess whether having a single point of governance or combining both security departments into a single department would benefit the organization more	• Assess if all security objectives are being accomplished by taking a closer look at the organizations' overall security policies. make modifications as technology changes, to provide a coherent future plan and direction for integrated security processes. • An initial convergence assessment should be done to identify current linked areas, possible gaps, vulnerabilities between security departments, and how these issues can be solved through convergence. • Key security experts and decision-makers should organize a convergence team to discuss the initial steps for the integration process. • Feasibility of resources should be taken into consideration while implementing convergence. There is not one size fits all when implementing convergence in security departments, and costs needs to be planned according to each rail operator capability and ecosystem.	• Ensure that the organization utilizes a single access security system for both physical and cybersecurity access by integrating security monitoring systems to prevent duplication of effort and to improve information flow. • Software and devices developed by vendors for the railway systems and operations should integrate security by design principles across all the development cycle. • Specific security certifications standards should be designed and required from service providers, to enhance the security level in the IT and OT railway systems and operations. • Decouple the whole security system on the network so that it may operate independently of the organization's general-use network, providing an additional layer of protection in the event of a general-use network security breach.

Figure 6: Recommendations for convergence of physical and cybersecurity in railways

7 Conclusion

Converged threats targeting critical infrastructures has increased in the last decade, and the railway networks are no exception. The deployed attacks against transportation cyber-physical systems are becoming more sophisticated and complex, making it difficult for railway operators to avoid and effectively deploy safety and security responses to both cyber and physical security environments simultaneously. The fast digital transformation the rail sector has been experiencing and the increased dependence on IP-connected devices in their core business have left their systems, operations, and infrastructure vulnerable to exploits.

This study has shown that Organization X and its members can improve their security operations and cost-efficiency through security convergence by eliminating siloed teams with

duplicated efforts, increasing their threat detection mechanism by closing communication and skills gaps. Furthermore, our findings show that by security convergence and developing a more holistic approach to security, Organization X and its members can strengthen their resilience against internal and external threats. Additionally, the convergence of Organization X members' security departments is an essential step to take full advantage of the benefits from new emerging technologies. With the implementation of the Industrial Internet of Things, cloud computing solutions, artificial intelligence, and consequently adopting the Industry 4.0 model in the railway operations, services, and infrastructure, these innovations are becoming part of the transformational new era for the rail industry.

Based on our research findings, we can conclude that to successfully design an effective convergence of the cybersecurity and physical security departments in the railway operations from Organization X' members. There needs to be a seamless integration of the three core elements of the business, namely, people, process, and technology.

We learned during our study that Organization X and its members can achieve a practical physical and cybersecurity integrated framework in their operations. By designing and implementing a clear holistic security strategy based on the organization ecosystem; upskilling and cross-training personnel, establishing intertwined communication channels for information sharing; and drawing up clear guidelines for converging security departments. Although the measures proposed in this thesis aims to assist Organization X's members in their security organizational structure's convergence implementation, each associate must tailor the integration of their security departments according to their reality and feasibility.

Some of the challenges we found while conducting our research were related to, that we only had access to general insights from the key stakeholder's interview about developing guidelines for integrating security departments in the railway sector; this was due to the sensitive nature of the information shared between Organization X and its members. We believe we would have benefited from more insights from other interviewees. More data from the other operators participating in the SAFETY4RAILS project would have contributed to gathering more information about the need to converge physical and cybersecurity environments in railway operations. However, considering the nature of Organization's X's international status as an entity, which promotes interoperability and needs' assessment from its worldwide members. They probably are exposed to vital information about the security needs of its members and may have valuable and concise insights and information about what they require to converge security environments effectively.

This thesis has demonstrated the actions needed to assist Organization X's members in developing a convergence implementation for their physical and cybersecurity environments. Our research can be a guideline or benchmark for future procedures designed to integrate

physical security and cybersecurity in the railway sector. Additionally, this study can be a starting point for further research related to the convergence of security departments in railways.

References

Printed sources

Yin, R.K. 2009. Case Study Research-Design and Methods. 3rd ed. Thousand Oaks. CA: Sage Publications.

Electronic

Adams, John., Khan, Hafiz TA & Raeside, Robert. 2013. Research Methods for Business and Social Science Students. New Delhi: SAGE Publications. E-book.

Arvis, J., Saslavsky, D., Ojala, L., Shepherd, B., Busch, C. and Raj, A., 2021. Connecting to Compete 2014: Trade Logistics in the Global Economy-The Logistics Performance Index and Its Indicators. Accessed June 13 2021. https://openknowledge.worldbank.org/handle/10986/20399

Baxter, P. and Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. The Qualitative Report Vol. 13 (4), 544-559. Accessed August 19 2021. https://doi.org/10.46743/2160-3715/2008.1573

Carlson, A., Frincke, D. & Laude, M., 2021. Railway Security Issues: A Survey of Developing Railway Technology. Accessed February 04 2021. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.565.2294&rep=rep1&type=pdf

Chen, B., Schmittner, C., Ma, Z. and Dong, X., 2015. Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective. Accessed February 01 2021. https://www.researchgate.net/profile/Christoph_Schmittner/publication/300144667

Cisa.gov. 2021. Cybersecurity and Physical Security Convergence - CISA. Accessed February 11 2021. https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021.pdf

Cobb, M., 2021. What is physical security? Search Security. Accessed June 15 2021. https://searchsecurity.techtarget.com/definition/physical-security

Contos, Brian T. 2007. Physical and Logical Security Convergence. Burlington: Massachusetts. E-book.

Cyber-physical Threats and Vulnerabilities Analysis for Train Control and Monitoring Systems. 2018. Rekik, M., Gransart, C. & Berbineau, M. International Symposium on Networks,

Computers and Communications June 2018. Hal Archives Ouvertes. Accessed February 15 2021. https://hal.archives-ouvertes.fr/hal-01852042/document

De Groot, J., 2020. What is Cyber Security? Definition, Best Practices & More. Online Digital Guardian. Accessed February 06 2021. https://digitalguardian.com/blog/what-cyber-security#:~:text=Cyber%20security%20refers%20to%20the,to%20as%20information%20technology%20security

USDA. 2021. Risk-Based Methodology for Physical Security Assessments. Accessed June 15 2021. https://www.dm.usda.gov/physicalsecurity/riskmanagementapproachpresentation.pdf

Encyclopedia. 2021. Modern Europe. British and Irish History. Railway. Accessed June 12 2021. https://www.encyclopedia.com/history/modern-europe/british-and-irish-history/railway

Flammini, F. 2012. Railway safety, Reliability, and Security. Scribd. Accessed February 04 2021. https://www.scribd.com/document/381173065/Francesco-Flammini-Francesco-Flammini-Railway-Safety-Reliability-and-Security

Gillham, Bill. 2000. Case Study Research Methods. Bloomsbury Publishing Plc. E-book.

Kothari, C.R. 2004. Research Methodology: Methods and Techniques. New Delhi: New Age International. E-book.

Kyllönen, M. 2012. 150 Years of Finnish Railways – Still a Vital Part of the Transport System. Global Railway Review. Accessed February 04 2021. https://www.globalrailwayreview.com/article/14723/

Lalonde, M. 2018. Combining Strengths: Cyber and Physical Security Convergence. Accessed February 08 2021. https://www.researchgate.net/profile/Melissa-Lalonde/publication/328964445_Combining_Strengths_Cyber_and_Physical_Security_Convergence/links/5bed80f54585150b2bb9ed27/Combining-Strengths-Cyber-and-Physical-Security-Convergence.pdf

Logan, K., Nelson, J., McLellan, B. and Hastin, A., 2020. Electric and hydrogen rail: Potential contribution to net zero in the UK. Accessed June 02 2021. https://doi.org/10.1016/j.trd.2020.102523

Monteagudo, J., 2021. Rail and Metro Cybersecurity. The First Global Cyber Security Observatory. Accessed June 18 2021. https://cyberstartupobservatory.com/rail-cybersecurity-where-is-the-industry-now/

Mulley, C., Hensher, D. and Cosgrove, D., 2017. Is Rail Cleaner and Greener than Bus? Accessed June 12 2021. https://doi.org/10.1016/j.trd.2016.12.004

Mutune, G., 2021. The Quick and Dirty History of Cybersecurity. Accessed June 16 2021. https://cyberexperts.com/history-of-cybersecurity

Safety4Rails. 2021. Safety4Rails Project. About. Accessed February 01 2021. https://safety4rails.eu

Shea, S., Gillis, A. and Clark, C., 2021. What is Cybersecurity? Everything You Need to Know. Search Security. Accessed June 15 2021. https://searchsecurity.techtarget.com/definition/cybersecurity

Staff, R., 2017. Fact box: Attacks on mass transit around the world. Accessed on April 05 2021. https://www.reuters.com/article/us-new-york-incident-attacks-subway-fact-idUSKBN1E52MN

Statistics Solutions. 2021. Choosing an Interview Type for Qualitative Research. Accessed August 05 2021. https://www.statisticssolutions.com/choosing-an-interview-type-for-qualitative-research/

Swedberg, R. 2020. C. Elman, J. Gerring, & J. Mahoney. Exploratory Research. The Production of Knowledge: Enhancing Progress in Social Science. Cambridge: Cambridge University Press. Accessed August 11 2021. https://www.cambridge.org/core/books/production-of-knowledge/exploratory-research/FD2ABFAD9DE34B44D015606C962A1AF0

Swinhoe, D., 2021. What is Physical Security? How to Keep your Facilities and Devices Safe from On-site Attackers. CSO Online. Accessed June 17 2021. https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html

Transportation Cyber-Physical Systems. 2018. Deka, Lipika. Chowdhury, Mashrur. Amsterdam: Elsevier. E-book.

Tyson, Dave. 2007. Security Convergence: Managing Enterprise Security Risk. Massachusetts: Butterworth-Heinemann. E-book.

UIC. 2021. Station Security for Station Business. Accessed June 16 2021. https://uic.org/IMG/pdf/station_security_for_station_business_handbook_2.pdf

Figures

Tables

Appendices

Appendix 1: Interview Questions

Interview Questions

1. What are Organization X's views on the need to integrate cybersecurity and physical security operations in the railway sector?
2. Are there surveys conducted by Organization X among its members about their needs regarding the convergence of physical security and cybersecurity?
3. To your knowledge, what actions/resources are currently available to railway operators to improve the security convergence in their operations?
4. What resources do railway operators have for structuring their physical and cyber security teams?
5. What are the tools available to railway's security teams, enhancing real-time information sharing among them?
6. In your opinion, what are the obstacles that could hinder the convergence of physical security and cybersecurity in railway operations?
7. In your opinion, what security's systems improvements vendors (e.g., third parties who manufacture the equipment's and machines used in the railway operations) could implement to provide more highly usable or user-friendly solutions to railway operators? How could the manufacturers assist in the integration of cyber and physical security in the railway?
8. In your opinion, what is the cross-training or further education needs that the staff may have to conduct to integrate physical and cybersecurity operations efficiently?
9. Do you think that the current standards like ISO 31000 and ISO 27001 provide sufficient guidelines for integrating cybersecurity and physical security?
10. Are there tools for conducting proper physical and cyber risk management outside of such standards like ISO 31000?
11. In your opinion, would legislation or regulatory framework play a big part in facilitating a broader adaptation of a converged physical and cybersecurity?
12. Can you describe the role artificial intelligence current plays in railway operators' security posture?
13. In your opinion, what are the requirements for railway operators to have an efficient integration of physical and cyber security operations?
14. Has it come to Organization X's attention the need to converge cyber and physical security operations in the railway sector to improve protection against hybrid security threats?
15. Is there any published material from Organization X related to the convergence of cyber and physical security departments?

Appendix 2: Interview Main Findings

Current Implementations to Integrate Security Departments	• Organization X have organized few meetings withs its members to discuss about the steps to converge the physical and cybersecurity departments in railways. Although, there were no further surveys or research to identify the measures needed to implement this integration. • The ongoing SAFETY4RAILS project is an excellent initiative to help the convergence in Organization X. The innovative platform will assist railway operators in the integration of security departments and provide tools to detect, prevent and mitigate the consequences caused by converged threats targeting the EU rail sector. • The outcomes from projects related to the safety and security in the railway sector are shared with the Organization X's members through their internal communication channels. Procedures related to physical security implementations and training are also available. Although guidelines dedicated to physical and cybersecurity convergence has not yet been published. • The physical security departments are usually responsibility of the corporative security, and the IT sector departments are the ones responsible to take care of the cyber security issues.
Challenges to Implement Convergence in Railway	• Most of the security departments from the railway operator's members belonging of Organization X, are siloed teams. • The converge implementation in the physical and cyber security departments in the railway operator's members are in different levels and stages. Some operators have more integrated departments than others. • The shortage of specialized professionals with expertise in cyber security skills dedicated to railway systems and network. The rail systems are very specific, such as the signalling systems in the tracks, and the railway operators are lacking this kind of professionals.
Resources Needed to an Effective Security Convergence	• Guidelines and frameworks to implement the steps to be followed for an effective convergence of security departments in railways. • More surveys and research related to the needs and challenges railway operators are experiencing to converge physical and cybersecurity departments. • Security by design should be implemented in each phase while developing devices and software for the rail sector. A certification in the product and a certification to integrate this product in the railway system, should be implemented also. • Artificial intelligence solutions had been implemented in some smart video surveillance in the railway sector, although this type of technology is still at the beginning of its application on the security sector and through the SAFETY4RAILS project, nfresh solutionsintegrating AI and the railway security departments will be developed.

Skills and Knowledge Required to Integrate Security Departments	• Physical and cybersecurity departments security staff should have regular cross-training to gain knowledge about the operations and procedures in both environments. • Integrated and clear communication channels between security departments should be implemented, where operational technology and informational technology systems are seamless connected and converged with security departments and decision makers.
Security Policies, Standards & Management Commitments	• Each country in the EU has its own legislations regarding the rail sector. Each European community member wants to maintain they own legislation and sovereign at national level, which can hinder the implementation of a legislation at European level. • The current available security standards and assessments are not designed for the challenging railway environment. They are more focused on the safety probability, instead of security likelihood. • Specific security standards based on the railway complex systems and environments are needed to effectively assess the risks • There are ongoing projects to develop specific standards focused on cyber security in railways. Although there is a lack of specific standards for risk assessment of physical and cybersecurity environments in railway systems and operations.