Cybersecurity in the Railway Sector

Simona Georgiana PREDESCU, Daniel SAVU, Victor Emmanuell BADEA
National Institute for Research & Development in Informatics - ICI Bucharest
simona.predescu@ici.ro, daniel.savu@ici.ro, emmanuell.badea@ici.ro

Abstract: This paper presents the approaches related to the digital transformation in the railway sector. Cyber security is a priority for the proper functioning of government or industrial control systems. Safety is a central point of the activities of the railway sector, being in the total responsibility of the companies, infrastructures and enterprises in the sector, while the security assurance is shared by them with the authorities. The most significant challenges facing this sector is cybersecurity. In recent years, railway companies have developed ambitious digital strategies, especially to cope with the growing number of passengers. They have implemented and interconnected information systems that combine IT, operational technology and the Internet of Things (IoT) in the management and control systems of trains, metro trains and trams, railway signaling systems and railway operations control centers.
Keywords: cybersecurity, railway, digital transformation, railway cybersecurity.

INTRODUCTION

Today, the digital transformation of business is a real challenge, especially for data security. The increasing complexity of IT systems and the development of multi-dimensional digital environments have led to the emergence of an increasing number of connected devices and communication channels between employees, customers, equipment and systems. Therefore, for an organization, the protection of its own information is an essential element for running a business in good conditions.

As organizations use more and more data and integrate reporting mechanisms and automated work processes into their day-to-day operations, the evaluation and protection of stored data is becoming increasingly important.

Currently, there is a significant difference between the volume of data generated daily that requires protection and the amount of data that is actually protected. This gap will widen so that by 2025, 90% of the world's existing digital data will need protection, but only half of it will be protected by its nature

https://doi.org/10.54851/v4i2y202210

(according to the Data Age 2025 Report, an IDC study sponsored by Seagate).

According to Romania's cyber security strategy, cyber security is the state of normalcy resulting from the application of a set of proactive and reactive measures to ensure the confidentiality, integrity, availability, authenticity and non-repudiation of electronic information, resources and public services. or private, from cyberspace (Braband, 2017).

Proactive and reactive measures may include security policies, concepts, standards and guidelines, risk management, training and awareness-raising activities, implementation of technical solutions for cyber infrastructure protection, identity management, consequence management.

Cyber security is a priority for the proper functioning of government or industrial control systems (production and distribution of electricity, water distribution, etc.). A cyber attack on a Supervisory Control and Data Acquisition System (SCADA) can result in loss of control, blockage, damage to facilities, or alteration of the final product. Often, incidents of this kind can have serious consequences such as a decrease in the level of security, the generation of economic and financial losses and the damage to the image of the organization (Mattioli & Moulinos, 2015).

The main elements of cyber security are:

- Confidentiality - Protecting and maintaining the confidentiality of information means ensuring that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.
- Integrity - In the context of computer systems, it refers to methods of ensuring that data is real, accurate and protected from unauthorized changes by the user.
- Access - Provides access to information and systems when needed. An example of an access issue is the DoS (Denial of Service) attack, in which attacks flood a user's system with network traffic to make accessing almost impossible. A ransomware attack encrypts a user's system and prevents a user from using it (BECHTEL, 2015).

The activity of critical sectors such as transport, energy, health and finance is increasingly dependent on digital technologies. Digitization offers huge opportunities and provides solutions to many of the challenges the world is facing, such as the crisis caused by the COVID-19 pandemic, but at the same time exposes economies and society to cyber threats.

Cyber attacks and cybercrime activities are becoming more numerous and sophisticated. The trend is to grow in the future, as there are forecasts that by 2024, 22.3 billion devices will be connected worldwide via the Internet of Things.

To create an open and secure cyberspace, a stronger cybersecurity response can increase citizens' trust in digital tools and services.

SAFETY AND SECURITY IN THE RAILWAY SECTOR

Safety is a central point of the activities of the railway sector, being in the total responsibility of the companies, infrastructures and enterprises in the sector, while the security assurance is shared by them with the authorities.

On the one hand, internally, the railway company manages the safety policy through a framework that involves human factors, events (safety, technical failures) and financial aspects (costs, benefits). On the other hand, security policy is structured through partnerships with national authorities. Railway actors focus on vulnerability issues and the level of threats is defined by the authorities. Because threats are constantly evolving, especially those related to cybersecurity, probability-based analyzes and cost-benefit approaches are less relevant than those aimed at protecting security.

Although different, safety and security requirements need to be consistent, as both safety risks and security threats can lead to unwanted events or accidents, resulting in serious damage and a high number of casualties.

In the railway sector, in the context of the adoption of state-of-the-art technologies, cyber security will become an essential component of business.

The existence, globally, of several digital projects in this sector, highlighted the need for integration with other modes of transport. Consequently, the railway community needs to open its businesses to players working in the field of multimodal transport solutions (Jablonski & Jablonski, 2022).

Ensuring information security requires compliance with requirements related to the operation of equipment with functions of control and maneuvering of rolling stock (systems and devices of automation and telemechanics for rail transport) and the installations (processes) of critical importance associated with them. These requirements relate to:

- Personnel and actors involved in the operation of automation and telemechanic systems and devices for rail transport;
- Physical protection;
- Access management;
- Data storage devices;
- Software;
- Intrusion detection;
- Response to information security incidents;
- Reliability.

IMPORTANCE OF CYBER SECURITY FOR THE RAILWAY SECTOR

Certainly, the digital age has brought a number of major benefits to the railway industry as a whole. However, the new opportunities may be discouraged by the large number of challenges facing the industry at the holistic level. In order to ensure the long-term reliability and sustainability of the railway sector, it is imperative that these challenges be countered and overcome.

The railway sector is facing a number of problems such as increasing competition from other modes of transport and the high costs of railway operations (Megan, 2019).

One of the most significant challenges facing this sector is cybersecurity. As most rail operations focus more on core functionality and accessibility, the rail sector has given marginal importance to ensuring cyber security until security breaches have multiplied and become public. As a result, national and local cybersecurity laws have become much stricter, with the railway sector having to comply with these regulations (Emilie & Christophe, 2017).

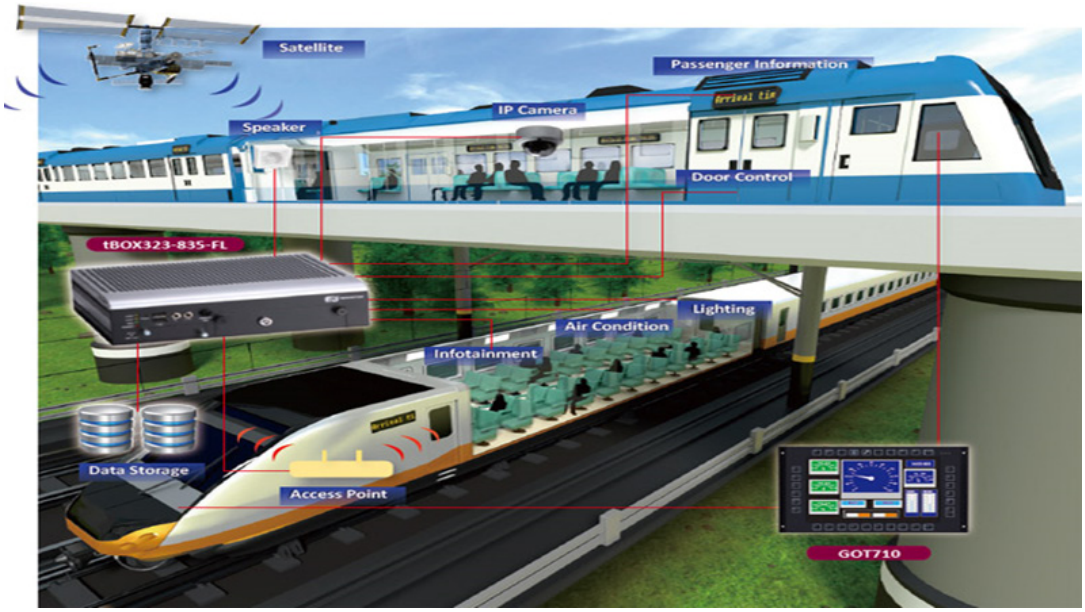

Fig. 1: *Intelligent railway safety oversight system (AXIOMTEK, 2015)*

The apparent inability of the railway sector to keep pace with technology is affecting the whole industry, and this key issue needs to be addressed at the decision-making level. Thus, the following must be taken into account:

- Technological progress;
- The life cycle of new information systems;
- Associated costs.

In the railway sector, there are real opportunities at the highest level of management of a company to address a multitude of different concerns related to cyber security.

Top management is responsible for cybersecurity across the organization, being involved in the proper protection of the company's assets and information.

In order to implement cybersecurity measures, senior management may delegate its responsibilities to other entities and is directly responsible for the validation of resource and investment requirements and the management of cybersecurity information (CEN, 2021).

CYBER SECURITY MEASURES ADOPTED BY ENISA (EUROPEAN UNION AGENCY FOR CYBERSECURITY) IN THE RAIL TRANSPORT SECTOR

Railway infrastructure and systems are essential assets of crucial importance for the development and security of the European Union. The railway sector plays an important role and is developing rapidly.

Due to the digitization of infrastructure, the automation of railway processes, the increase in the number of activities related to mass transport and the interconnection with other external and multimodal systems, the railway sector is undergoing major transformations in terms of its operations, systems and infrastructure. This sector is also evolving as it gradually opens up to competition, by reallocating responsibilities and separating railway systems and infrastructure, which also directly affects information technology systems. In this context, it is increasingly important to address cyber threats in the railway sector (Liveri et al., 2020).

The railway sector provides transport of goods and passengers within and outside a country's borders. The main actors in this sector are:

- Railway companies. They offer freight and passenger services.
- Infrastructure managers. Deal with:
  - » traffic management;
  - » management of control and signaling systems;
  - » creation, management and maintenance of railway infrastructure and fixed installations;
  - » supply of rolling stock with fuel and electricity.

These actors fall within the scope of the NIS Directive (EU Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on the adoption of measures to ensure a high level of security of networks and information systems in the European Union) and the identification of as essential service operators (ESOs) comply with the transposition of the Directive into the laws of the Member States.

Currently, the implementation stage of the NIS Directive for essential service operators in the railway sector is as follows:

- The widespread implementation of security measures dedicated to governance and the ecosystem is heterogeneous and slow compared to the implementation of other types of measures. These security measures are already applied by most essential service operators with experience in the field. However, for less experienced service providers, the implementation of these measures is in its infancy.
- Protective measures to ensure security are best implemented. Although the basic elements of cyber security are effectively implemented, the level of implementation of security measures that require advanced technical expertise is lower. In the special context of operational technology, in terms of factual issues, number of systems, vendor dependency and security issues, it is often impossible to implement basic security without applying compensatory countermeasures.

- With regard to defensive security measures, a number of basic security measures are already in place and effective, such as ways to communicate with relevant authorities and cyber security incident response teams. However, as they require considerable expertise, large-scale cybersecurity measures are being implemented to a lesser extent.
- The level of implementation of resilience measures is considered to be good. In the railway sector, crisis and incident management is part of the daily routine. However, there are still opportunities for improvement by addressing new cyber security threats in existing crisis management and resilience processes.

Regarding the implementation of the NIS Directive, the main challenges facing the railway sector are the following:

- As the railway sector is undergoing a digital transformation, stakeholders in this field need to strike a balance between operational requirements, business competitiveness and cyber security.
- Stakeholders in the railway sector depend on providers with different technical standards and cyber security capabilities, especially in terms of operational technology.
- Over time, operational technology in the railway sector has been based on a number of systems considered to be secure, in line with the technical state at the time. However, due to their long lifespan, these systems have become obsolete or morally worn out, making it difficult to update them to today's cyber security requirements. In addition, these systems are usually spread over a network of railway stations, tracks, etc., which makes it difficult to ensure a comprehensive level of cyber security.
- Due to cultural differences, there is a low level of awareness among railway operators, especially operational staff and those involved in the application of security measures, of the need to ensure cyber security.
- The existing specific railway regulations do not include provisions on cyber security. Essential service operators often have to comply with non-harmonized cyber security requirements arising from different regulations (Liveri et al., 2020).

Fig. 2: *Security measures for essential service operators (AXIOMTEK, 2015)*

GLOBAL RAILWAY SECURITY CYBER SECURITY MARKET FORECAST 2021-2027

In 2021, the railway cybersecurity market is estimated to have reached $ 6.2 billion and will reach $ 10.6 billion by 2027, at a compound annual growth rate (CAGR) of 9.4%. 2021-2027. In this sector, the use of the Internet has led to the creation of smart cities, smart transportation, rail traffic management systems, train control systems via radio communications (CBTC) and Positive Train Control (PTC) systems. Advanced technologies include Passenger Information System (PIS), intelligent ticketing systems, passenger info-infotainment, rail analysis, cloud services and the Internet of Things, freight information and analysis, solutions such as fleet monitoring, automatic inventory management, smart devices and scheduling and optimization capabilities. However, all these technologies face cyber security threats. In the railway industry, due to the advent of advanced systems and solutions, the Internet of Things is more prone

to cyber security threats. In the railway sector, all these factors lead to the need to increase the number of implementations of cyber security solutions (MarketsandMarkets, 2022).

Increasing the number of data security breaches and data leaks has an impact on the market for cybersecurity products, solutions and services. Advances in technology are often accompanied by an increase in the number of automated and sophisticated cyber attacks. Globally, the increasing sophistication of cyber attacks has led rail operators to adopt a range of cyber security solutions and services in order to combat them. For example, in France in May 2021, the French National Railway Company (SNCF) and its partners Alstom, Bosch, SpirOps, Thales and the Railenium Research Institute announced that they would begin developing an autonomous train prototype. As cybersecurity is a key concern of the utmost importance for its realization, since the beginning of the project the consortium partners have collaborated with the National Agency for Security of Information Systems (ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information), the French national authority for cyber security. In order to find the best cybersecurity solutions for the rail market, in 2020, Alstom invested $ 7 million in the Israeli company Cylus, which specializes in cybersecurity.

Within this sector, the implementation of smart digital systems requires joint efforts by various stakeholders, such as telecommunications operators, infrastructure providers, service providers, manufacturers, the public sector and user groups. For the implementation and financing of transport projects, government authorities have adopted public-private partnership (PPP) models, which allow private sector companies to participate in government initiatives dedicated to smart, digital and connected rail transport. This has an important impact on the demand for cyber security projects in the railway sector.

The Asia Pacific region is the fastest growing area of the cyber security market in the railway sector. The governments of the countries in this region are collaborating with companies specialized in information technology and cyber security for the large-scale implementation of driverless train technology. In 2020, the fastest driverless train in the world was launched in China.

Fig. 3: *Opportunities in the cyber security market in the rail transport sector (MarketsandMarkets, 2022)*

The new driverless high-speed train linking the Chinese cities of Beijing and Zhangjiakou is capable of reaching a top speed of 350 km / h, making it the fastest autonomous train in the world in operation. These trains are equipped with a range of security systems, entertainment systems and other state-of-the-art systems that require cyber security solutions. As the number of high-speed rail programs in China has increased, so has the investment in infrastructure and dedicated digital equipment. High-speed railways operate in different infrastructures and are therefore based on sophisticated communication and management solutions. As a result, increasing the adoption rate of high-speed trains worldwide will help accelerate the demand for cyber security solutions (Cheshire, 2016).

IMPACT OF COVID-19 ON THE CYBER SECURITY MARKET

The outbreak of the COVID-19 pandemic prompted major rail component manufacturers/ solution providers to announce the suspension of production/supply of services due to declining demand, supply chain bottlenecks and to protect employee safety. In 2020, the COVID-19 pandemic led to a decrease in the demand for passenger and freight transport, which further aggravated the already existing delays related to the implementation of cyber security projects in the railway sector. In addition, budget allocations for research and development have been significantly affected, which has affected innovative developments in this sector.

To a large extent, the demand for railway cyber security solutions depends directly on government budgets (Alexe et al., 2017).

Globally, rail traffic has been severely affected by the COVID-19 pandemic. According to the Deutsche Bahn, due to coronavirus restrictions, the use of long-distance and regional passenger trains has fallen to 15% of normal demand. Due to the decrease in cargo volume, trains were loaded to about 70% of their normal capacity. The pandemic also led to delays in some railway projects, especially in India, where the duration of the restrictions was very long. Companies such as Alstom and Thales reported significant losses in terms of revenue from the railway business. In the short term, the pandemic is expected to have a significant impact; however, the railway industry is expected to recover and grow strongly over the next five years. Growth could be accelerated by significant investments in Very High Speed (VHS) and High Speed (HS - High Speed) railway infrastructure.

Due to the pandemic, the cost of purchasing solutions for the railway sector, such as management systems, is minimal. The emergence of new waves of COVID-19 is expected to further affect the cost of railway cyber security solutions due to the declining revenues of railway operators.

CYBER ATTACKS ON THE RAILWAY SECTOR

Although this sector has not been a direct target for cybercriminals so far, a number of cyber attacks and incidents have taken place, highlighting its vulnerability. The following is a detailed list of the most well-known incidents that have taken place in the European Union and other European countries:

- 2015, Ukraine - DoS attack. An APT (Advanced Persistent Threat) APT has carried out a large-scale coordinated attack to destabilize the Ukrainian government. This type of actor is usually a state or state-sponsored group that gains unauthorized access to a computer network and remains undetected for a long time. Currently, the term also refers to groups not sponsored by a state that carry out large-scale targeted intrusions for specific purposes. In Ukraine, the attack targeted power plants, mining facilities and railway infrastructure. Its purpose was to paralyze public and critical infrastructure by disabling industrial control systems (ICS).
- July 2015 - July 2016, Great Britain - intrusion attack. Between July 2015 and July 2016, four cyber attacks were identified on the UK rail network. After analyzing them, it was considered that these attacks were part of a reconnaissance operation before an APT-type attack, probably led by a threatening state actor. No data interruptions or changes were detected.

- May 2017, Germany - ransomware attack. Deutsche Bahn, Germany's largest rail passenger and freight, logistics and network technology company, has fallen victim to WannaCry ransomware. Some devices have been corrupted and as a result could no longer display passenger information. Train traffic was not interrupted.
- October 2017, Sweden - DDoS attack. The first attack took place on 11 October and affected the Swedish Transport Administration (Trafikverket) through its two internet service providers, TDC and DGC. The DDoS attack appears to have affected IT systems that monitor the location of trains. The government agency's e-mail system, website and road maps were also targeted. During this time, customers were unable to make reservations or receive updates regarding delays. As a result, train traffic and other services were managed manually, using back-up processes. The next day, a second DDoS attack affected the website of the Swedish Transport Agency, an independent government body responsible for regulating and inspecting transport systems. The public transport operator Vasttrafik in western Sweden was also attacked, affecting the ticketing application and the online travel planning service.
- May 2018, Denmark - DDoS attack. A DDoS attack has affected the ticketing systems of DSB (Danske Statsbaner), a Danish rail passenger company. Danish passengers were unable to buy tickets from ticket vending machines, the online application, the website and some of the railway station counters. The DSB estimated that about 15,000 customers were affected.
- March 2020, United Kingdom - data breach attack. The email addresses and travel details of the approximately 10,000 people who used the free Wi-Fi provided by UK stations were displayed online. Network Rail, the UK railway infrastructure manager and service provider C3UK have confirmed the incident. The database contained 146 million records, including personal contact details and birth dates. Another violation involved the „Indian Rail" app, which is a top app in Apple's App Store, as a Firebase database was exposed. Violation included 2,357,684 emails, usernames and passwords in plain text.
- May 2020, Switzerland - malware attack. Swiss rail car maker Stadler has been hit by a malware attack that has affected all its premises and allowed attackers to steal sensitive company data. After compromising Stadler's systems, the attackers infected its systems with malware that was then used to extract sensitive corporate data from the attacked systems. The internal documents stolen during the cyber attack on Stadler's premises were published online after the manufacturer refused to give in to the ransom requests.
- July 2020, Spain - ransomware attack. ADIF, the Spanish railway infrastructure manager, suffered a ransomware attack which, although it did not affect critical infrastructure, exposed gigabytes of personal and business data (Kour et al., 2019).

CONCLUSIONS

Cybersecurity starts to have a major impact in the railway sector. Employees of operational staff must carry out tasks falling within the scope of their official duties, provided that such tasks do not infringe established access rights and do not compromise the security of information. It is recommended that the purchase of equipment and software for automation and telemechanics for rail transport, including data protection hardware and software, be carried out only if they are accompanied by up-to-date documents certifying compliance with the conditions laid down in the technical documentation. Telecommunication cables and connection systems, as well as the local networks that are part of these systems, must be designed in accordance with the rules laid down for the technical design of automation and telemechanics.

Local networks, which include channels and lines of communication, must be made in accordance with the design documentation. Radio equipment in automation and telemechanics for rail transport must be registered on the basis of the compliance documentation. Access to data storage devices should be allowed only to authorized persons included in a list. The number of these people should be as small as possible. People who are not listed do not have access to these devices (NOKIA, 2020).

Ensuring the protection of data storage devices against unauthorized access involves defining procedures. Thus, devices must be registered and labeled so that they can be unambiguously identified. The locations of the devices and their children must be accurately determined. The backups must be stored in a place other than the one where the main storage devices are located.

The transport of data storage devices must be controlled and handled only by authorized persons. In the railway sector, the assignment of responsibilities involves a multitude of actors, such as divisions and departments that share responsibilities related to ensuring cyber security at the industry level. The responsibilities are different depending on the abilities of each actor.

For example, asset owners share responsibilities for rail management, risk mitigation, and network management. System integrators are responsible for access management, technical evaluation, and system architecture. Suppliers are responsible for the reliability of the final product and software components as well as the overall security of the manufacturing processes.

If electronic data storage devices are to be transferred for off-site use of the automation and telemechanic systems for rail transport, they must first be formatted. The steps for formatting the device must be monitored and documented. Data storage devices that will no longer be used in the future must be decommissioned.

ENISA has recently outlined (ENISA Railway Cybersecurity - Security measures in the Railway Transport Sector, November 2020) a variety of cyber security concerns as they are felt by infrastructure or train operators. These include the fact that employees pay less attention to digitalization and cyber security, the link between cyber security and passenger safety, the digital transformation of the key business processes, or the reliance on the degree of security of the products and services offered by the entire supply chain.

REFERENCE LIST

Alexe, L., Pereira, H., Ribeiro, P. Marques, F., & Bonneau, M.-H. (2017). *CYbersecurity in the RAILway sector. D2.1 – Safety and Security requirements of Rail transport system in multi-stakeholder environments* (EU Project 730843). Retrieved from https://projects.shift2rail.org

AXIOMTEK (2015). *Trends in Factory Automation: The Internet of Things.* Retrieved from http://www.axiomtek.it/Download/Article/Download/trends_factory_automation_%20IoT_091115.pdf

BECHTEL (2015). *Cybersecurity for Public Transportation Rail Systems – The Bechtel Approach*. Retrieved from https://www.bechtel.com/getmedia/f0ec1853-243c-4445-9e62-968a1ce37faa/Cybersecurity-for-Transportation-Rail-Systems_v2_final.pdf

Braband, J. (2017). Cyber Security in Railways: Quo Vadis?. In A., Fantechi, T., Lecomte & A., Romanovsky (Eds.). *Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - Second International Conference - RSSRail 2017*, Pistoia, Italy, 3-14. DOI: 10.1007/978-3-319-68499-4_1

CEN (European Committee for Standardization). (2021). *A major step for railways cybersecurity: the new CLC/TS 50701.* Retrieved from https://www.cencenelec.eu/news-and-events/news/2021/eninthespotlight/2021-06-10-new-clc-ts-50701-railways-cybersecurity/

Cheshire, T. (2016). *Four Cyber Attacks On UK Railways In A Year.* Retrieved from https://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558

Émilie, M., & Christophe, G. (2017). CyberSecurity for Railways – A Huge Challenge – Shift2Rail Perspective. In A., Pirovano, M., Berbineau, A., Vinel, C., Guerber, D., Roque, J., Mendizabal, H., Bonneville, H., Aniss & B., Ducourthial (Eds.). *Communication Technologies for Vehicles: 12th International Workshop, Nets4Cars/Nets4Trains/Nets4Aircraft 2017*, Toulouse, France. Lecture Notes in Computer Science.

ENISA (2020). *Railway Cybersecurity - Security measures in the Railway Transport Sector.* Retrieved from https://www.enisa.europa.eu/publications/railway-cybersecurity/@@download/fullReport

Jabłoński, A., & Jabłoński, M. (2022). *Digital Safety in Rail Transport – Basic Assumptions.* Springer Series in Reliability Engineering, Springer.

Kour, R., Karim, R., & Thaduri, A. (2019). Cybersecurity for railways – A maturity model. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 234*(10), 1129-1148. DOI: 10.1177/0954409719881849

Liveri, D., Theocharidou, M., & Naydenov, R. (2020). *Railway Cybersecurity - Security measures in the Railway Transport Sector*. ENISA (European Union Agency for Cybersecurity) https://www.enisa.europa.eu/publications/railway-cybersecurity/@@download/fullReport

MarketsandMarkets (2022). *Railway Cybersecurity Market by Type (Infrastructural & On-board), Offering, Security Type (Network, Application, Endpoint, System Administration and Data Protection), Application (Passenger & Freight), Rail Type and Region - Global Forecast to 2027*. Retrieved from https://www.marketsandmarkets.com/Market-Reports/railway-cybersecurity-market-128598673.html

Mattioli, R., & Moulinos, K. (2015). *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors.* ENISA (European Union Agency for Cybersecurity) https://www.enisa.europa.eu/publications/maturity-levels

Megan, E. (2019). *Why is cyber-security so important for the rail industry.* Retrieved from https://www.globalrailwayreview.com/article/77240/cyber-security-paradigm-rail-sector/

NOKIA (2020). *Cyber security for railways.* Retrieved from https://www.nokia.com/networks/solutions/cyber-security-for-railways/>railways-cybersecurity/