



Article

A Novel Security Risk Analysis Using the AHP Method in Smart Railway Systems

İsa Avcı ^{1,*}  and Murat Koca ² ¹ Department of Computer Engineering, Faculty of Engineering, Karabuk University, Karabuk 78050, Turkey² Department of Computer Engineering, Faculty of Engineering, Van Yuzuncu Yil University, Kampüs, Tuşba, Van 65080, Turkey; muratkoca@yyu.edu.tr

* Correspondence: isaavci@karabuk.edu.tr

Abstract: Transportation has an essential place in societies and importance to people in terms of its social and economic aspects. Innovative rail systems need to be integrated with developing technologies for transportation. Systemic failures, personnel errors, sabotage, and cyber-attacks in the techniques used will cause a damaged corporate reputation and revenue losses. In this study, cybersecurity attack methods in smart rail systems were determined, and cyber events occurring worldwide through these technologies were analyzed. Risk analysis in terms of transportation safety in smart rail systems was determined by considering the opinions of 10 different experts along with the Analytic Hierarchical Process (AHP) performance criteria. Informatics experts were selected from a group of people with at least 5–15 years of experience. According to these risk analysis calculations, cybersecurity stood out as the most critical security risk at 27.74%. Other risky areas included physical security, calculated at 14.59%, operator errors at 16.20%, and environmental security at 10.93%.

Keywords: smart railway system; smart railway transportation; cybersecurity; AHP risk analysis



Citation: Avcı, İ.; Koca, M. A Novel Security Risk Analysis Using the AHP Method in Smart Railway Systems. *Appl. Sci.* **2024**, *14*, 4243. <https://doi.org/10.3390/app14104243>

Academic Editors: Helge Janicke, Leandros Maglaras and Mohamed Amine Ferrag

Received: 9 April 2024

Revised: 7 May 2024

Accepted: 11 May 2024

Published: 16 May 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Technology development has increased significantly, digitalizing communication, transportation, control, and security systems. All kinds of management, maintenance, comfort, and safety procedures used in rail systems are organized and developed according to international norms and are interrelated thanks to specific physically or virtually connected infrastructure. There has been an increase in digital technologies with an innovative approach in the rail system sector, with the development of digitalization in existing infrastructure and an increase in new lines and locations.

The concepts of intelligent transportation and smart railway systems have become trending topics for all critical infrastructure and industrial control systems, like the smart grid concept introduced in recent years. In addition, smart cities are based on restructuring cities to maximize human and natural productivity by reducing their complexity. In addition, smart grids and cities use a human-oriented, strategic management approach that creates and supports development, change, and the environment. These cities are urban spaces with improved service areas and living standards. The structures within these cities are based on creating comfortable, healthy, human-oriented, self-sufficient living spaces where innovative and sustainable methods are applied efficiently and intelligently, respecting nature and minimizing environmental problems [1]. Smart railway systems, like these systems, have features that facilitate human life, increase comfort, provide safe transportation, and save time.

In terms of existing infrastructure and developments, while there was no HST (High-Speed Train) line before 2009 in Turkey, it has reached a length of approximately 1213 km, and the total length of the rail system is 12,740 km. According to the TCDD (the Republic of Turkey State Railways) 2020 Performance Program, Logistics, and Transportation sector

forecast, the HST line length will be 5595 km by 2023 [2]. In addition to the development of the rail system in our country, the use of railway system transportation, which is one of the safest transportation methods used for freight and passenger transportation in the world, is predicted to increase by 40% by 2040, according to the international Railway Delivery Group data.

These developments require academic and industry-oriented studies to keep up with the development of digital technologies and to eliminate the cybersecurity risks that arise with this technology. In view of global industry developments, new needs arise. The most important company in the transport sector is TCDD, which has started to build railway infrastructure as a necessary development. Official sources and reports of TCDD's strategies and developments show that TCDD has begun to carry out many important studies regarding the integration of data systems and the inclusion of digital systems in the transportation sector. The survey carried out within the Eskisehir Regional Directorate Digital Transformation Office of TÜRASAŞ, which is one of the affiliate institutions of TCDD, shows that the development of digitalization infrastructure has begun, from industry 4.0 applications to the application of all kinds of digital technologies, and it was transformed into a test station. These and similar studies aim to ensure the development of smart transportation infrastructure in railway systems in our country.

The development of ITS also paves the way for cybersecurity vulnerabilities. ITS applications are also similar to cyber-attacks, depending on the applications used. Cyber-attacks, especially those on web-based applications, have similar attack vectors. The difference here is that attacks such as communication-based listening, changing information on information screens, and infiltrating control units are possible in ITS traffic lights, signs, control systems, and road applications.

The use of intelligent transportation systems in railway transportation provides convenience in preventing accidents and operational and system safety. However, errors and accidents can occur in cases of systemic malfunctions, errors, and cyber-attacks, which are observed worldwide and may occur in smart transportation systems. In the last 15 years, it has been observed that nearly 200 people have lost their lives in rail transportation systems due to various reasons, especially signaling system errors. In addition, the use of multi-criteria decision-making methods for rail transportation systems is discussed in the literature [3]. Our study will examine the basic infrastructure architectures and communication systems of smart rail systems. Together with these examinations, the affected systems will be prioritized, and the events that have occurred or may occur will be evaluated in detail.

2. Smart Railway System and Used Communication Structures

Developments in digital technologies, smart transportation, and railway systems have made it possible to control all kinds of controllable systems of vehicles and stations with physical and virtual connections. The control of these systems from specific centers contributes to their protection from possible accidents, malfunctions, data loss, time and income loss, and the formation of more efficient new designs and structures with the experience gained.

Railway systems carry cargo and passengers between cities. Many different systems are monitored by control centers. Infrequent applications, station control centers, sub-control centers from the main control center, and vehicle and road systems (such as line security systems, point, and signaling systems) are controlled by communication infrastructures such as LANs (Local Area Networks), Fiber Optics, 4G, and 5G. Depending on the design of the railway station and the length of the railway route, different station control systems and track systems are used, which are controlled from the main control center [4]. The network architecture of substation control centers and vehicle controls managed from the main control center is shown in Figure 1.

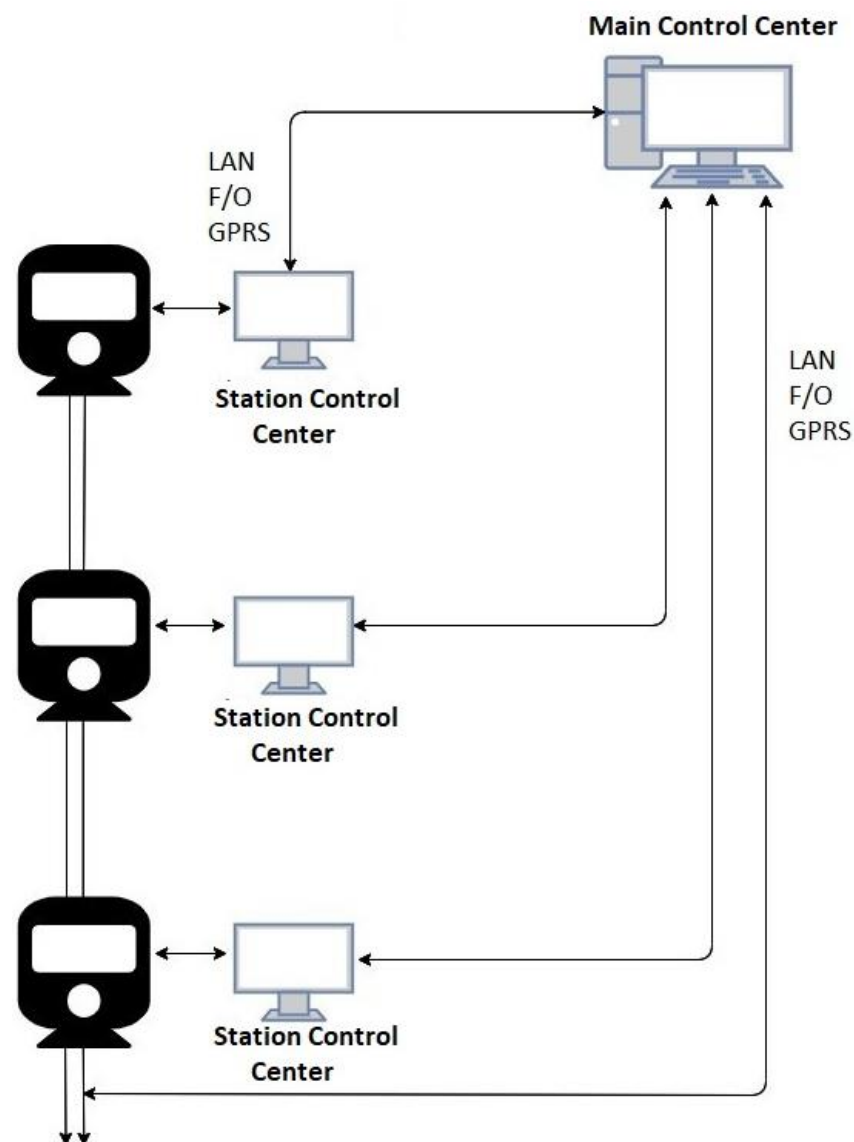


Figure 1. Main control network architecture in smart railway systems.

It provides control of vehicle navigation, security, control, and comfort systems by communicating with the developed main control centers and station control systems. Lighting, stairs, ventilation, cameras, elevators, ticket control, and security systems, which are among the station's control, security, and comfort systems, are controlled. Apart from the station, vehicle movement, security, comfort, control systems, switches, signals, and road control systems are maintained. In Figure 2, the structure of the systems controlled by the station control systems communicating with the main control center inside and outside the station is shown.

All kinds of comfort, navigation, and driving systems are managed on the rail system vehicles operated from the primary and station control centers. While these systems control all passenger systems, they also carry out the necessary cruise planning and movement operations by communicating with the center during the cruise. The systems controlled on the rail system vehicle are shown in Figure 3.

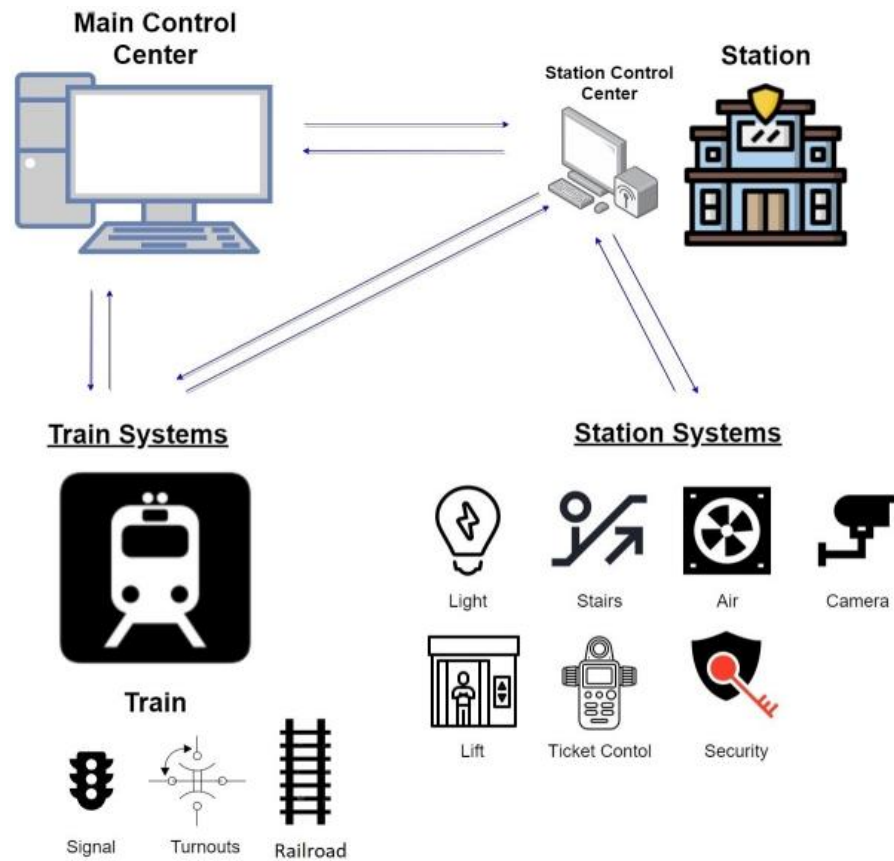


Figure 2. Systems station control center in smart railway systems.

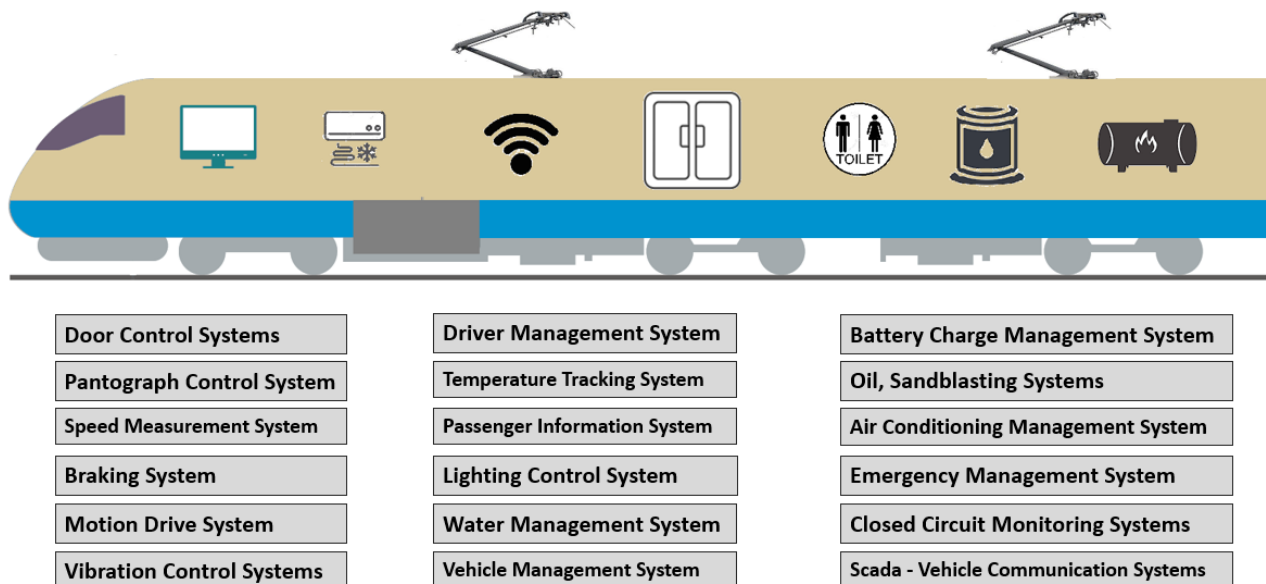


Figure 3. Vehicle-controlled systems in intelligent railway systems.

3. Cybersecurity in Smart Railway Systems

The cyberspace environment refers to environments in which all kinds of information exist. These environments include every environment, from transportation to health to the defense industry to the food industry. The masses of information revealed by the cyberspace environment mean cybersecurity applications need to be protected from threats to ensure their sustainability.

With the commercial use of the internet in the 1990s, usage started to increase, and in 2021, it had more than 4 billion users. This user presence has made it standard for internet environments to be insecure with security gaps and increased security risk. “Critical infrastructures” are among the most critical things that cybersecurity systems deal with. Critical infrastructures are summarized as structures that cause loss of life and property because of the deterioration or accessibility of existing information and reveal security vulnerabilities on a national scale [5].

Data processing and the use of these data are among the necessary operations, as well as the protection of the data. While the development of existing technologies is provided by digital technology, it will reduce the security problems and time losses related to this field that we will encounter in the future, without further cybersecurity vulnerabilities. Every day, billions of people rely on railways and metros to navigate rapidly growing and increasingly congested countries and cities. Digitalization increases connectivity, and automation makes our trains faster, safer, more comfortable, and more punctual. However, it also makes them vulnerable to cyberattacks. Railway system services can be severely disrupted; customer data can be stolen, causing severe economic damage. Even the safety of passengers is under significant threat [6,7]. It is vital to protect our railways with advanced, high-tech cybersecurity solutions. The focus should go beyond just trying to prevent and detect attacks and react quickly [8].

The purpose of implementing cybersecurity measures is to ensure the integrity of systems by protecting a computer system or group of computers from attempts to break into a scheme or network and from attempts to steal, alter or destroy stored information. These cyber-attacks come from sources that are difficult to track and generally take different forms depending on how they infect, reproduce, and damage viruses, worms, bots, or software [9].

3.1. Systems Affected by Cyber-Attacks in Smart Railway Systems

With the development of digital technologies in smart railway systems, brakes, air conditioning, cameras, sensors, etc., electronic systems continue to be at risk from cyber-attacks. In addition to these systems, non-vehicle systems are also at risk [10]. Non-vehicle systems can be listed as infrastructure-related central control systems, sub-control systems, network systems, communication and communication systems, and signaling systems. Potential systems at risk of cyber-attacks in smart railway systems are presented in Figure 4 [11].

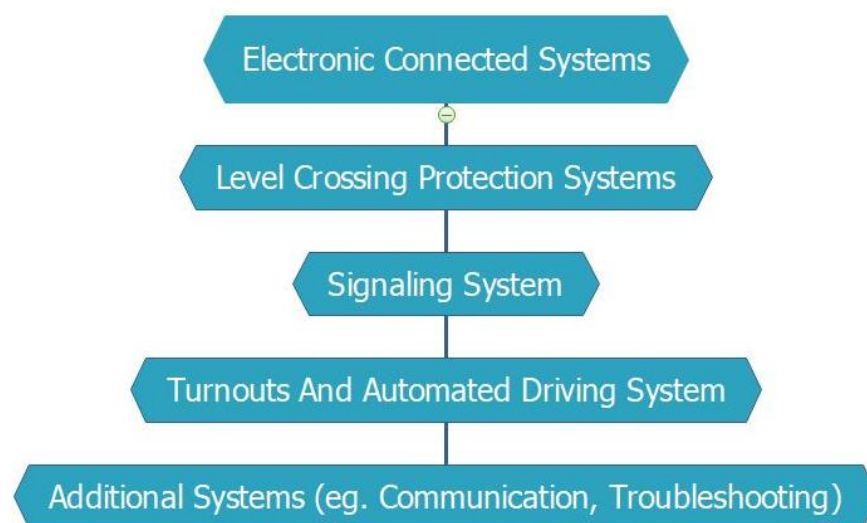


Figure 4. Potential systems at risk of cyber-attacks in smart railway systems.

3.2. Cyber-Attack Incidents and Attack Methods Experienced in Smart Railway Systems

Worldwide research on smart railway systems, institutions, equipment, and attack methods has identified those that have experienced cyber-attacks. There have been a few instances where security problems have arisen in the smart railway system industry [12]. These are listed below in Table 1.

Table 1. Cyber-attack incidents experienced in smart railway systems [12].

Year	Location	Cyber Incident
2008	Poland	In Lodz, Poland, a person derailed four tram trains with his television remote.
2011	US—Northwest Region	A group of hackers attacked remote computers, and the train signal system in the northwest region of the United States was stopped for two days.
2013	Belgium	NMBS (Belgian National Railway) accidentally published the personal information of several customers.
2014	Japan	Japan Airlines confirms the information of frequent flyer program members was stolen.
2014	USA—New York	Data on several million trips in a year by passengers using New York taxis were published.
2015	North Korea-Seoul	Pirates infiltrated the subway system in Seoul, North Korea.
2016	US—San Francisco	The hard disk of ticket systems was encrypted by a ransomware attack in San Francisco.
2017	Sweden	The Swedish Transport Agency leaked some driver information to Eastern Europe due to illegal data access in IBM systems.

When the smart railway transportation systems were examined, the most commonly experienced or likely cyberattack methods were investigated, as listed below [13,14]. These can be cyber-attacks in communication and communication systems used in rail transportation, network systems, software and hardware, electrical and electronic systems, mechanical systems, and signaling systems. Cyber-attack methods are presented in Figure 5 [15,16].

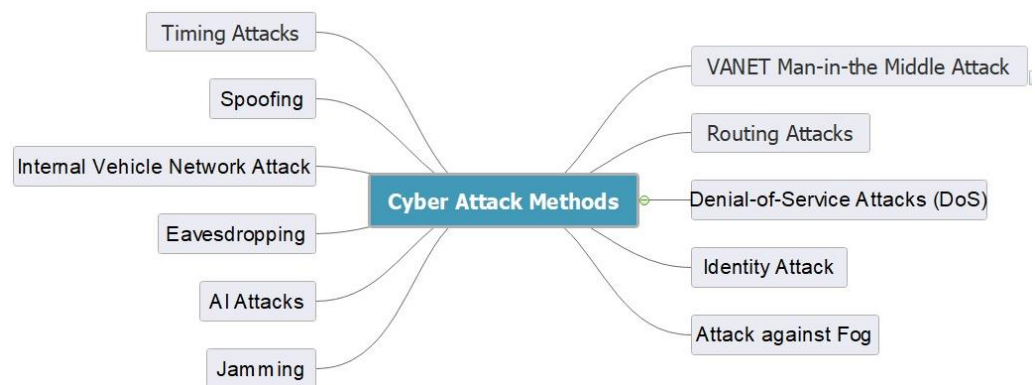


Figure 5. Cyber-attack methods in smart rail systems.

The cybersecurity attack methods identified in the research have been determined to be commonly experienced and possible attacks. As the number of systems data increases, it becomes more challenging to protect and control them. With the developing technologies, the vulnerability of big data in terms of security causes data to be disclosed, stolen, and lost, with consequences for corporate reputation and revenue. For this reason, cyber-attack methods have been determined by researching smart railway systems. Security measures should be taken at the highest level for all smart systems used against these cyber-attacks.

3.3. Security Risk in Smart Railway Systems

With the widespread use of digital technologies in smart railway transportation systems in recent years, hardware and software security problems have increased [17]. Security risks that can be experienced in smart railway systems are detailed below. These security risks have occurred in past events and may arise in the future.

- Collisions in trains;
- Derailment;
- Train disruption;
- Frequent interruptions in train services;
- A situation that leads to fear and possible loss of life;
- A condition causing the passengers discomfort;
- The public being harmed by threats to the safety of the workforce, passengers, or personnel;
- Financial loss;
- Criminal damage;
- Failure to comply with the law;
- Loss of reputation and leakage of sensitive information in railway systems.

The security risks mentioned here should be evaluated as risks that can be experienced in terms of security that smart railway systems will be exposed to. The loss of life, property, and income is inevitable in these events. Therefore, more secure models should be preferred when taking steps to ensure the safety of the systems [18,19].

4. Material and Methods

The Analytical Hierarchy Process (AHP) was first introduced by the Myers and Alpert duo in 1968. In 1977, it was developed as a model by Saaty and made usable for solving decision-making problems. The AHP can be explained as a decision-making method. The estimation method used in the decision hierarchy can be defined and gives the percentage distribution of decision points in terms of factors affecting the decision. The AHP is based on one-to-one comparisons of the factors affecting the decision and the essential values of the decision points in terms of these factors, using a predefined comparison scale on a decision hierarchy. Consequently, differences in significance turn into percentage distribution over decision points. The comparison matrix between elements is a $n \times n$ square matrix. The matrix components on the diagonal of this matrix take the value 1. The comparison matrix is shown below in Equation (1) [20].

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \quad (1)$$

Comparisons are made for all values above the diagonal of 1 in the comparison matrix. Naturally, for the components below the diagonal, it will be sufficient to use the formula in Equation (2).

$$a_{ji} = \frac{1}{a_{ij}} \quad (2)$$

Considering the example given above, if the first-row, third-column component of the comparison matrix ($i = 1, j = 3$) takes the value 3, the third-row, first-column component of the comparison matrix ($i = 3, j = 1$) will take the value $1/3$ from the formula. The AHP significance scale makes a binary comparison. AHP significance levels are shown in Table 2.

Table 2. AHP importance rates.

Importance Values	Value Definitions
1	When both factors are of equal importance.
3	When the 1st factor is more important than the 2nd factor.
5	When the 1st factor is more important than the 2nd factor.
7	When the 1st factor has extreme importance compared to the 2nd factor.
9	When the 1st factor has superior importance compared to the 2nd factor.
2,4,6,8	Intermediate values.

Comparisons of patching selection performance criteria show two sequential performance indicators that intersect each cell. Additionally, each value is shown in a different table by dividing the column totals. Also, the averages of the obtained values were calculated. The normalized binary comparison matrix is shown in Equation (3).

$$B_i = \begin{bmatrix} b_{11} \\ b_{21} \\ \cdot \\ \cdot \\ b_{n1} \end{bmatrix} \quad (3)$$

Also, binary comparisons allow for precise subjective evaluation criteria. Consistency queries help with the evaluation provisions made by binary comparison. Here, patch management application selection criteria are evaluated using performance criteria appropriately designed under the AHP. Additionally, these evaluations were carried out by many experts in the information technology sector. Weighted average evaluations were calculated according to expert opinions. The normalized binary comparison matrix formula is shown in Equation (4).

$$b_{ij} = \frac{a_{ij}}{\sum_{i=1}^n a_{ij}} \quad (4)$$

5. Risk Analysis of Cybersecurity and Physical Threats in Smart Railway Systems

Various losses of property and life may occur in rail system operations due to not taking the necessary precautions and measures. These errors, which may arise due to human origin and the installed infrastructure and systems, can lead to insecurity of the course to be carried out, financial losses, and the loss of corporate reputation. Basic critical security may be required based on railway system structures' vehicle travel and road conditions. Especially for routes with a single road in our country (the existing railway infrastructure between two stations is one-way, and incoming and outgoing vehicles use the same roads), SCADA errors, systemic errors, infrastructure errors, operator errors, machinist errors, or cyber-attacks cause accidents with profound consequences. A traceable and controllable system must be installed correctly to ensure security in smart railway systems. The smooth operation of this system and the analysis and planning of security measures should be ensured to protect against possible attacks [21].

Cyber-attacks, terrorist attacks, sabotage, employee errors, and machine and material errors in the installed and operating systems should be prevented. Safe models should be created by considering these situations. These models should be adapted to national and international standards, thereby ensuring environmental safety and physical security, and preventing financial damage and loss of corporate reputation [22]. Domestic resources that are not dependent on external sources should be used to control the system correctly. Transportation safety in smart rail systems is explained in Figure 6.

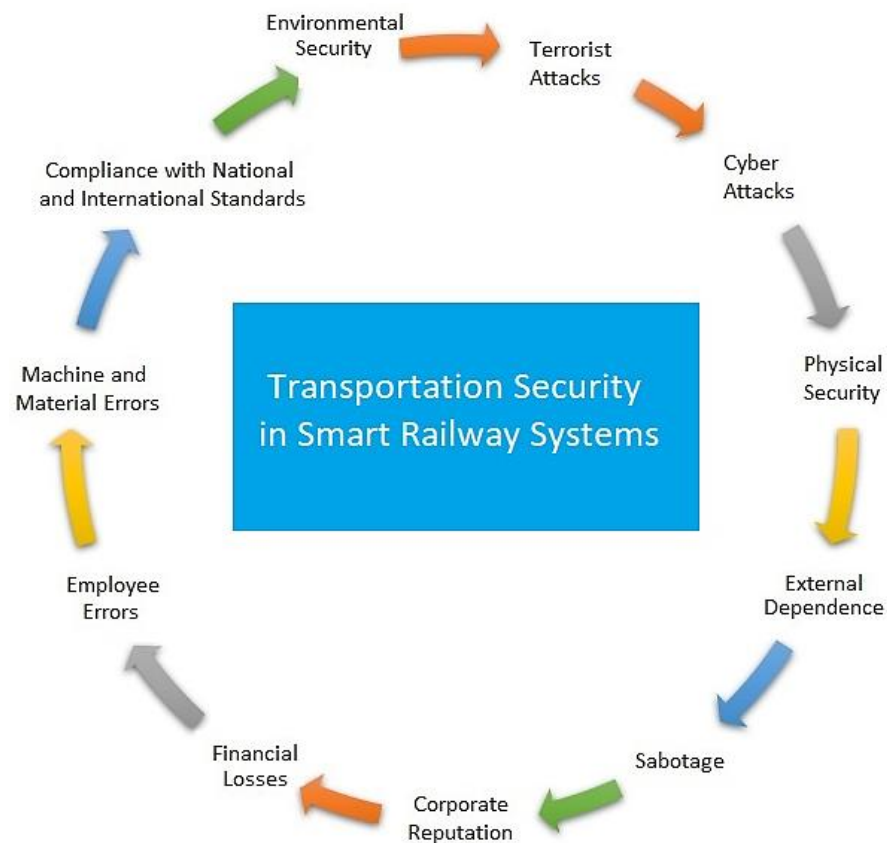


Figure 6. Key performance indicators of security in smart railway systems.

Smart railway systems depend on many criteria to ensure safe transportation in the transportation security model. When they are investigated, especially in data security, it is essential to address cybersecurity, employee errors, and physical security. On the other hand, in addition to all of these, environmental safety and climatic conditions are also essential [23,24]. It is possible to determine the effect values of these given criteria in terms of risk by considering expert opinions. Also, all systems must be aligned with national and international standards [25,26].

Risk Analysis Results

According to expert opinions, a risk analysis was carried out by making calculations with the AHP method. Risk value parameters in smart railway systems were obtained by interviewing individuals who are experts in their fields because of research. Risk analyses were carried out based on these parameters. In this study, all data was created by considering the areas of expertise. Therefore, we believe that the data obtained will be valuable for academic studies and institutions in the sector. The AHP method is based on the pairwise comparison method and is used to determine which is the most important risk. Risk situations in smart railway systems are discussed and revealed with the calculation results obtained within the scope of this study, and it is seen that there are differences between these results and the real risk. The main reasons for this include the rapid development of technologies, increased investments, and the high rate of use by society compared to previous years. For this reason, to fully reveal the risks, this study is the first to determine which risks are of higher priority and importance. In this research article, the results of all calculations are given in Tables 3 and 4. The data in Table 3 were calculated with the values in Table 2 according to the calculations given in Formulas (1) and (2).

Table 3. Security risk key performance indicators in smart railway systems.

Smart Railway Systems KPIs	Cybersecurity	Physical Security	Operator Errors	Environmental Security	Terrorist Attacks	Machine and Material Errors	Sabotage	Corporate reputation	Material Damages	Standards	Foreign Dependence
Cybersecurity	1	8	7	8	8	5	7	6	9	9	9
Physical Security	0.12	1	6	8	5	3	3	9	5	5	7
Operator Errors	0.14	0.16	1	9	9	9	9	9	9	6	8
Environmental Security	0.12	0.12	0.11	1	8	9	6	7	7	5	7
Terrorist Attacks	0.12	0.200	0.11	0.12	1	9	8	7	6	7	7
Machine and Material Errors	0.20	0.33	0.11	0.11	0.11	1	5	7	7	5	7
Sabotage	0.14	0.33	0.11	0.16	0.12	0.20	1	5	5	5	5
Corporate Reputation	0.16	0.11	0.11	0.14	0.14	0.14	0.20	1	5	4	9
Material Damages	0.11	0.20	0.11	0.14	0.16	0.14	0.20	0.20	1	9	8
Standards	0.11	0.20	0.16	0.20	0.14	0.20	0.20	0.05	0.11	1	8
Foreign Dependence	0.11	0.14	0.125	0.14	0.14	0.14	0.20	0.11	0.12	0.12	1
Totals	2.36	10.81	14.95	27.03	31.83	36.82	39.80	51.36	54.23	56.12	76

Table 4. Normalized importance weight order of key performance indicators in smart railway systems.

Smart Railway Systems KPIs	Cybersecurity	Physical Security	Operator Errors	Environmental Security	Terrorist Attacks	Machine and Material Errors	Sabotage	Corporate Reputation	Material Damages	Standards	Foreign Dependence	Norm. Totals	Norm. Total Percent Value
Cybersecurity	0.42	0.74	0.47	0.30	0.25	0.14	0.18	0.12	0.17	0.16	0.12	3.05	27.74
Physical Security	0.05	0.09	0.40	0.30	0.16	0.08	0.08	0.18	0.09	0.09	0.09	1.61	14.59
Operator Errors	0.06	0.02	0.07	0.33	0.28	0.24	0.23	0.18	0.17	0.11	0.11	1.78	16.20

Table 4. *Cont.*

Smart Railway Systems KPIs													
	Cybersecurity	Physical Security	Operator Errors	Environmental Security	Terrorist Attacks	Machine and Material Errors	Sabotage	Corporate Reputation	Material Damages	Standards	Foreign Dependence	Norm. Totals	Norm. Total Percent Value
Environmental Security	0.05	0.01	0.01	0.04	0.25	0.24	0.15	0.14	0.13	0.09	0.09	1.20	10.93
Terrorist Attacks	0.05	0.02	0.01	0.00	0.03	0.24	0.20	0.14	0.11	0.12	0.09	1.02	9.31
Machine and Material Errors	0.08	0.03	0.01	0.00	0.00	0.03	0.13	0.14	0.13	0.09	0.09	0.73	6.64
Sabotage	0.06	0.03	0.01	0.01	0.00	0.01	0.03	0.10	0.09	0.09	0.07	0.48	4.40
Corporate Reputation	0.07	0.01	0.01	0.01	0.00	0.00	0.01	0.02	0.09	0.07	0.12	0.41	3.71
Material Damages	0.05	0.02	0.01	0.01	0.01	0.00	0.01	0.00	0.02	0.16	0.11	0.38	3.46
Standards	0.05	0.02	0.01	0.01	0.00	0.01	0.01	0.00	0.00	0.02	0.11	0.23	2.05

Table 4. Cont.

Smart Railway Systems KPIs	Cybersecurity	Physical Security	Operator Errors	Environmental Security	Terrorist Attacks	Machine and Material Errors	Sabotage	Corporate Reputation	Material Damages	Standards	Foreign Dependence	Norm. Totals	Norm. Total Percent Value
Foreign Dependence	0.05	0.01	0.01	0.01	0.00	0.00	0.01	0.00	0.00	0.00	0.01	0.11	0.97
Totals	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	11.00	100.00

The risks in terms of the smart railway transport sector were divided into 11 categories. While determining these categories, the opinions of the institution, experts in the industry, and academic experts were taken into consideration. At the same time, risk performance criteria were determined by examining national and international educational studies. In addition, national and international standards on smart railway systems were reviewed, and contributions were made to this study. Scores ranged between 1 and 9 according to the AHP method used to evaluate smart railway transportation systems, which was examined under 11 categories. According to this grouping, a binary comparison was made between risks, and their significance levels are given in Table 3. After the values in this table were computed with the AHP method, normalized values were calculated according to Table 4 for each risk value. Then, according to the AHP method, the normalized total values for the specified risk and the significance weights as a percentage were determined according to the normalized total value. The results in Table 4 were created by normalizing the data in Table 3 using Formulas (3) and (4).

According to the calculations of the parameters obtained for smart railway transportation systems, the risk importance ranking is given in Table 5. According to this ranking, each risk’s importance has been pointed out. In addition, representations in a radar graph are shown in Figure 7. The data in Table 5 summarize the normalized values in Table 4.

According to these risk importance calculations, when looking at other parameters after cybersecurity, physical security stands out at 14.59%, operator errors are at 16.20%, and environmental security is at 10.93%.

The radar chart shows the weakest and strongest attack methods that can be experienced. This graph shows the risk significance values obtained from the calculations made with the AHP method. Among these risks, cybersecurity is the most striking risk, with a rate of 27.74%.

Table 5. Security risk key performance indicators’ importance weight order in smart railway systems.

Smart Railway Systems KPIs	Importance Weights (%)
Cybersecurity	27.74
Physical Security	14.59
Operator Errors	16.20
Environmental Security	10.93
Terrorist Attacks	9.31
Machine and Material	6.64
Sabotage	4.40
Corporate Reputation	3.71
Material Damages	3.46
Standards	2.05
Foreign Dependence	0.97
Totals	100.00

Security Risk Analysis in Smart Railway Systems

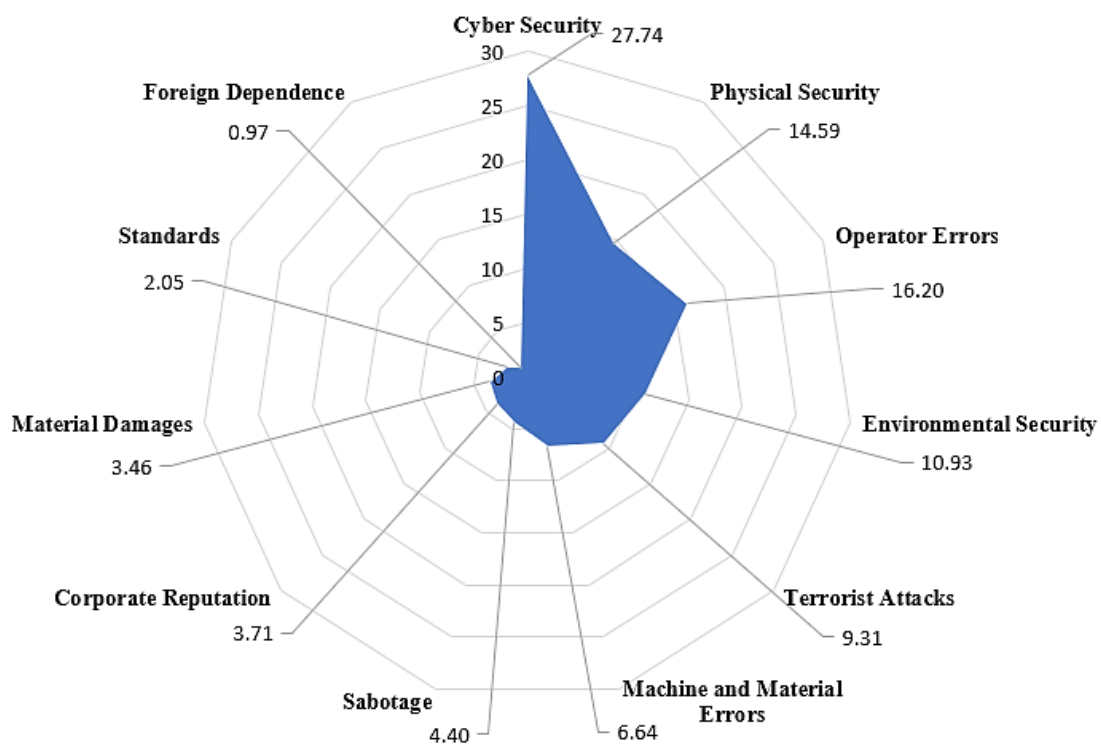


Figure 7. Security risk analysis in smart railway systems: importance weight values presented in radar graph.

6. Conclusions

Technological developments in smart railway transport systems contribute to the economic and social development of the region. Rail systems are preferred because they balance the load in other transportation systems and are more effective in certain areas. Considering the competitive sector, supporting railway systems will contribute to sustainable structures in the long run. Simultaneously with the infrastructure investments in developing countries, technological investments in smart railway systems are increasing rapidly. Researchers should put forward strategic studies to support the safe, effective, and

efficient use of smart railway system technologies. Approaches and solutions using information and communication technologies should be developed to solve the transportation problems of smart railway systems. Creating a safer traffic flow and an environmentally friendly transportation environment by making the communication between people, vehicles, and infrastructure smart is necessary. With the rapid development of technologies in smart railway systems, security problems in these systems have come to the forefront. The increasing cybersecurity attacks in recent years also pose a risk to these systems.

In this study, the factors affecting the safety of smart railway systems were determined, and a risk analysis of these factors was conducted with the AHP method. The risk analysis in terms of transportation safety in smart railway systems was carried out by considering ten different expert opinions along with the “Analytical Hierarchical Process (AHP)” performance criteria. The experts who were consulted were selected from those who have at least 5–15 years of experience in the sector. According to these risk calculations, cybersecurity came to the forefront as the most critical security risk at 27.74%. Other risky areas included physical security, calculated at 14.59%, operator errors at 16.20%, and environmental security at 10.93%. According to the risk analysis performance indicators determined in this study, cyber-attacks are more critical than other performance indicators. According to the risk analysis study, it is necessary to take more effective security measures against cybersecurity attacks on the systems used in smart rail systems. These attacks will result in loss of income and reputation, data loss, and loss of life and property for organizations. Physical security risk ranks second after cybersecurity when looking at other risk analysis performance indicators. Specific strategies should be developed to protect, design, and support smart railway systems. In addition, safe models should be developed in which all systems can work together.

Author Contributions: Conceptualization, İ.A.; methodology, İ.A.; software, M.K.; validation, İ.A., and M.K.; resources, İ.A.; data curation, M.K.; writing—original draft preparation, M.K.; writing review and editing, İ.A.; supervision, İ.A. All authors have read and agreed to the published version of the manuscript.

Funding: The research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors reported no potential conflicts of interest.

References

1. Avcı, I.; Ozarpa, C.; Aydın, M.A. A survey of international security standards for smart grids, industrial control system and critical infrastructure. In Proceedings of the 12th International Exergy, Energy and Environment Symposium (IEEES-12), Doha, Qatar, 20–24 December 2020; pp. 421–424.
2. Çelebi, D. Supporting rail freight services in Turkey: Private sector perspectives on logistics connectivity issues. *Case Stud. Transp. Policy* **2023**, *14*, 101098. [[CrossRef](#)]
3. Tomić, V.; Marinković, D.; Marković, D. The Selection of Logistic Centers Location Using Multi-Criteria Comparison: Case Study of the Balkan Peninsula. *Acta Polytech. Hung.* **2014**, *11*, 97–113. [[CrossRef](#)]
4. Tekteş, N.; Tekteş, M. Future goals of intelligent transportation systems in the world examination of japan sample. *PARADOKS Econ. Sociol. Policy J.* **2019**, *15*, 189–210.
5. Topaloglu, S. Modeling of Public Relations (PR) Strategies for Cyber Threat Management. Doctoral Dissertation, Mykolo Romerio Universitetas, Vilnius, Lithuania, 2023.
6. Mecheva, T.; Kakanakov, N. Cybersecurity in intelligent transportation systems. *Computers* **2020**, *9*, 83. [[CrossRef](#)]
7. Verhulsdonck, G.; Weible, J.L.; Helser, S.; Hajduk, N. Smart cities, playable cities, and cybersecurity: A systematic review. *Int. J. Hum. Comput. Interact.* **2023**, *39*, 378–390. [[CrossRef](#)]
8. Sharma, R.; Rajeev, A. Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4571. [[CrossRef](#)]
9. Del Moral, J.; iOlius, A.D.; Vidal, G.; Crespo, P.M.; Martinez, J.E. Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. *arXiv* **2024**, arXiv:2401.03780.

10. Bonde, D.; Pawar, P.; Patekar, S.; Mane, R.; Pawar, S. Smart railway system for safe transportation. *OAIJSE* **2018**, *3*, 83–85.
11. Hasan, M.; Habib, A.A.; Shukur, Z.; Ibrahim, F.; Islam, S.; Razzaque, A. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *J. Netw. Comput. Appl.* **2023**, *209*, 103540. [[CrossRef](#)]
12. Lamssaggad, A.; Benamar, N.; Hafid ASMSahlı, M. A survey on the current security landscape of intelligent transportation systems. *IEEE Access* **2021**, *9*, 9180–9208. [[CrossRef](#)]
13. Xie, J.; Zhang, S.; Wang, H.; Chen, M. Multiobjective network security dynamic assessment method based on Bayesian network attack graph. *Int. J. Intell. Comput. Cybern.* **2024**, *17*, 38–60. [[CrossRef](#)]
14. Göçoğlu, V. Cyber security of critical infrastructures in smart cities. *Uluslararası Yönetim Akad. Derg.* **2019**, *2*, 51–63. [[CrossRef](#)]
15. Jadoon, A.K.; Wang, L.; Li, T.; Zia, M.A. Lightweight cryptographic techniques for automotive cybersecurity. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1640167. [[CrossRef](#)]
16. Hahn, D.A.; Munir, A.; Behzadan, V. Security and privacy issues in intelligent transportation systems: Classification and challenges. *IEEE Intell. Transp. Syst. Mag.* **2019**, *13*, 181–196. [[CrossRef](#)]
17. Kelarestaghi, K.B.; Foruhandeh, M.; Heaslip, K.; Gerdes, R. Intelligent transportation system security: Impact-oriented risk assessment of in-vehicle networks. *IEEE Intell. Transp. Syst. Mag.* **2019**, *13*, 91–104. [[CrossRef](#)]
18. Ralston, P.A.; Graham, J.H.; Hieb, J.L. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans.* **2007**, *46*, 583–594. [[CrossRef](#)] [[PubMed](#)]
19. Abdo, H.; Kaouk, M.; Flaus, J.M.; Masse, F. A safety/security risk analysis approach of industrial control systems a cyber bowtie combining new version of attack tree with bowtie analysis. *Comput. Secur.* **2018**, *72*, 175–195. [[CrossRef](#)]
20. Saaty, T.L. Scaling method for priorities in hierarchical structures. *J. Math. Psychol.* **1977**, *15*, 234–281. [[CrossRef](#)]
21. Avcı, I.; Ozarpa, C.; Aydın, M.A. Mitigating global warming in smart energy grids via energy supply security for critical energy infrastructure. *Int. J. Glob. Warm.* **2021**, *25*, 288–305. [[CrossRef](#)]
22. Yan, Z.Y.; Chun, Z.J.; Liu, G.J.; Zou, L.L. Risk Analysis of Cyber Security in Nuclear Power Plant. In *Innovative Technologies for Instrumentation and Control Systems*; SICPNPP 201; Lecture Notes in Electrical Engineering; Springer: Singapore, 2017; Volume 455.
23. Thaduri, A.; Aljumaili, M.; Kour, R.; Karim, R. Cybersecurity for eMaintenance in railway infrastructure: Risks and consequences. *Int. J. Syst. Assur. Eng. Manag.* **2019**, *10*, 149–159. [[CrossRef](#)]
24. Ozarpa, C.; Aydın, M.A.; Avcı, I. International security standards for critical oil, gas, and electricity infrastructures in smart cities: A survey study. In *Innovations in Smart Cities Applications*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 4, Chapter 89; pp. 1167–1179.
25. Gombár, M.; Vagaská, A.; Korauš, A.; Račková, P. Application of Structural Equation Modelling to Cybersecurity Risk Analysis in the Era of Industry 4.0. *Mathematics* **2024**, *12*, 343. [[CrossRef](#)]
26. Avcı, I.; Ozarpa, C.; Biçer, Y. Supply security in critical energy infrastructures for reliable energy grids. In Proceedings of the 12th International Exergy, Energy and Environment Symposium (IEEES-12), Doha, Qatar, 20–24 December 2020; pp. 293–297.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.