Informatics and Software Engineering
p-ISSN/e-ISSN: 2988-2818/2988-2222
Homepage: https://sanscientific.com/journal/index.php/ise
3**(1) 9-19 (2025)**
https://doi.org/10.58777/ise.v3i1.253

Research Article

LRT System Security Analysis: Threats and Solutions for Implementation in Indonesia

Rizqi Mustafa Maulana[1], Zaki Azfa AlHafiz[2], Syahzana Agfah[3], Nurbo Jatmiko[4]
[1] Sistem Informasi, Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta
[2] Sistem Informasi, Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta
[3] Sistem Informasi, Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta
[4] Sistem Informasi, Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta

Received: December 22, 2024; Revision: April 3, 2025;
Accepted: April 9, 2025; Available Online: April 30, 2025;

Abstract
The security of the Light Rail Transit (LRT) system is a significant concern as its utilization continues to grow in Indonesia. As a viable solution to urban congestion, the LRT encounters various challenges, including cyberattacks and technical issues that could disrupt operations and jeopardize passenger safety. This study aims to analyze these threats and propose solutions using the ISO-31000:2018 framework. The research employs a Systematic Literature Review (SLR) methodology to assess risks based on their likelihood and potential impact. The findings indicate that the primary threats include phishing attacks, ransomware, and signal system failures. However, this study has limitations, as it is based exclusively on secondary data, which may not fully reflect local conditions. The originality of this research lies in its application of ISO-31000:2018 within the local context and its provision of practical recommendations for operators and policymakers. Moreover, it paves the way for future studies to conduct more comprehensive, field-based research.

Keywords: *LRT System security, Risk management, Threats and solutions*

How to cite: Maulana, RM., Alhafiz, ZA , & Agfa, S. LRT System Security Analysis: Threats and Solutions for Implementation in Indonesia. *Informatics and Software Engineering*, *3*(1). https://doi.org/10.58777/ise.v3i1.253

*Corresponding author: nurbojatmiko@uinjkt.ac.id

1. Introduction

The security of the Light Rail Transit (LRT) system is a significant concern as its utilization continues to grow in Indonesia. As a viable solution to urban congestion, the LRT encounters various challenges, including cyberattacks and technical issues that could disrupt operations and jeopardize passenger safety. This study aims to analyze these threats and propose solutions using the ISO-31000:2018 framework. The research employs a Systematic Literature Review (SLR) methodology to assess risks based on their likelihood and potential impact. The findings indicate that the primary threats include phishing attacks, ransomware, and signal system failures. However, this study has limitations, as it is based exclusively on secondary data, which may not fully reflect local conditions. The originality of this research lies in its application of ISO-31000:2018 within the local context and its provision of practical recommendations for operators and policymakers. Moreover, it paves the way for future studies to conduct more comprehensive, field-based research.

However, as LRT usage increases, safety becomes a major concern for operators and users. Maintaining LRT system security is a complex challenge as it involves a variety of threats, ranging from criminal acts such as theft and vandalism to more serious threats such as terrorist attacks and cyberattacks. These threats can not only cause material losses but also threaten the safety of passengers and the reputation of the transportation system itself.

Jumlah Penumpang	Jumlah Penumpang Light Rail Transit (LRT) Jakarta (Orang)											
	2024											
	Januari	Februari	Maret	April	Mei	Juni	Juli	Agustus	September	Oktober	November	Desemb
Jumlah Penumpang	93.631	89.934	92.004	84.571	96.550	102.707	-	-	-	-	-	

Figure 1: LRT Passenger Count Data

According to recent data, the number of LRT users in Indonesia is expected to continue increasing by 2024. This increasing graph shows the public's confidence in the LRT system as a reliable and efficient mode of transportation. However, this increase in ridership also means an increase in security risks for LRT operators. Security analysis of Light Rail Transit (LRT) systems in Indonesia reveals significant vulnerabilities and potential threats, particularly from terrorism and cyber-physical attacks. Addressing these issues requires a multifaceted approach that includes risk assessment methodologies, physical protection systems and the application of advanced technologies. The following sections outline key aspects of security threats and solutions for LRT systems. This research underlines that the integration of information technology in transportation systems can minimize security risks (Purwani et al., 2024).

Safety is critical in Light Rail Transit (LRT) systems as they transport a large number of passengers every day (Hakim, 2024). Ensuring passenger safety helps build public trust and encourages more people to use public transportation, which can reduce congestion (Kemmala, D., & Aris, K. 2023) in urban areas such as Jakarta. To address these safety challenges, a comprehensive and sustainable approach is needed (Sarjito et al. 2023), (Putri et al. 2025). Security solutions should include preventive measures (Soleh, M., & Tjenreng, Z. 2025), early detection, rapid response and post-incident recovery. In addition, active participation from various stakeholders, including the government (Firmansyah, M., & Yuswanto, A. 2022), LRT operators, law enforcement, and the community, is necessary to create a safe and comfortable transportation environment.

This research aims to identify the main threats to LRT system security in Indonesia and evaluate the solutions that have been implemented or have the potential to be implemented. We use mixed methods, combining quantitative and qualitative data analysis to provide a comprehensive picture of the current LRT security situation. The results of this study are expected to provide practical recommendations that can be used by LRT management to improve passenger safety and comfort.

2. Literature Review

2.1. Light trail Rail (LRT)

Light Rail Transit (LRT) is a public transportation system that offers an effective solution to congestion in big cities. Compared to other public transportation, LRT has the advantage of faster operations due to dedicated lanes that are not affected by traffic congestion. According to (Sianturi et al., 2025), the implementation of LRT can reduce dependence on private vehicles, reduce congestion, and improve air quality in urban areas. It also has a positive impact on the economy by improving accessibility to key areas, such as business centers.

However, despite its benefits in reducing congestion, LRT development requires large investments and a lengthy construction process, as described by Wang et al. (2017). Challenges in financing and infrastructure management are major obstacles for cities to utilize the potential of LRT optimally.
According to (Putri, N. H. A., and Sahara, 2023), LRT can improve the quality of life of city residents by reducing travel time and improving mobility. Moreover, integration between LRT and other modes of transportation, such as buses and trains, can increase the overall transportation efficiency of the city.

2.2. Systematic Literature Review

Systematic Literature Review (SLR) is an approach used to collect, evaluate and analyze existing literature related to a research topic in a systematic and structured manner. The aim is to develop a comprehensive synthesis based on the available evidence objectively and transparently (Kitchenham, 2004). SLR involves an organized series of steps, from the formulation of the research question to the synthesis of the findings.

This process includes an extensive literature search and rigorous selection based on pre-determined inclusion and exclusion criteria, as outlined by Moher et al. (2009). The key steps in SLR, including planning, searching, quality evaluation and extraction of relevant data, were all undertaken to ensure that the resulting review was valid and accountable.

2.3. Cyber Security in LRT Systems

Cybersecurity in the LRT system is a crucial aspect that needs attention. According to research by Kharisma et al. (2024), public transportation systems are highly vulnerable to cyber attacks such as ransomware and DDoS attacks. In Indonesia, this threat is increasing along with the development of technology and the integration of IoT in LRT operations. This research examines the different types of cyberattacks that may occur and the solutions that can be implemented to mitigate these risks.

3. Methods

This research uses a qualitative approach with the Systematic Literature Review method to analyze threats and solutions to LRT system security in Indonesia. SLR was chosen because it provides a systematic framework for identifying, evaluating, and synthesizing relevant literature in a transparent and structured manner. The main objective of this research is to provide a description and expression of the security threats and solutions that can be done to overcome these threats. The data obtained in this research was collected through a literature review of scientific journals, news articles, industry reports, and transportation security standards. This research also uses the ISO-31000: 2018 Framework as an action to see important aspects of risk management. The stages of this research include:

3.1. Research Stages

a. Problem Identification
   This stage is the first step in carrying out research, which consists of knowing the background of the problem, determining the formulation of the problem, determining the scope or limitations of the problem, determining the objectives of the research, and determining the benefits of the research. This stage aims to make researchers understand the application of the ISO-31000: 2018 Framework as a means of analyzing risk and understanding the case study object to be studied.
b. Literature Study

The researcher conducted a systematic search of relevant literature, including scientific journals, industry reports, books and transportation safety standards. This process aimed to gain in-depth insight into the threats faced by LRT systems, risk mitigation practices and the application of risk management frameworks. Literature sources were selected based on inclusion criteria such as topic relevance, source validity and publication quality.

c. Data Analysis
The data obtained from the literature was organized based on the ISO 31000:2018 Framework, with a focus on:

1. Communication and Consultation: Identifies the importance of communication and stakeholder engagement in risk management.
2. Define Scope, Context and Criteria: Analyze the scope of LRT security risks, including physical and cyber threats, and establish risk criteria based on likelihood and impact.
3. Risk Assessment: Mapping the risks identified through the desk study into an assessment framework, including an in-depth analysis of the impact and likelihood of threats to the LRT infrastructure.
4. Risk Treatment: Identify relevant mitigation strategies, such as strengthening security infrastructure, implementing AI-based technology, and improving system operating procedures.
5. Monitoring and Review: Evaluate the results of the literature study to ensure compatibility with the conditions of the LRT system in Indonesia.

d. Conclusions and Suggestions
The final stage involves drawing conclusions that summarize the key findings from the literature, including the threats faced by LRT systems and suggested mitigation measures. Recommendations are provided for LRT operators, regulators, and further researchers to explore more innovative and specific solutions.

4. Results

4.1 Establishment of Context Scope and Criteria
The scope of this research focuses on risk management in the Indonesian LRT system using the ISO-31000:2018 framework. The main objective is to identify and analyze the various risks that exist in the current LRT operational system to evaluate whether it is running according to the expected safety standards or whether obstacles can hinder the smooth operation of transportation services.

The analysis was conducted by establishing a risk criterion based on two main parameters: frequency of occurrence (likelihood) and risk impact (impact) on LRT operations. The likelihood parameter is divided into five levels, which can be seen in Table X: Rare, Unlikely, Possible, Likely, and Certain.

Table 1. Risk criterion based

Criteria	Information	Frequency	Value
Rare	Very rare risk	>3 Years	1
Unlikely	Infrequent risk	2-3 Years	2
Possible	Risk sometimes occurs	1-2 Years	3
Likely	Risk of frequent occurrence	7-12 Month	4
Certain	Risk is bound to happen	<7 Month	5

Meanwhile, the impact parameter is also divided into 5 levels, as can be seen in Table 2: Insignificant (Very Small Impact), Minor (Small Impact), Moderate (Medium Impact), Major (Large Impact), and Catastrophic (Very Large Impact).

Table 2. The impact parameter

Criteria	Information	Value
Insignificant	Risk does not interfere with the company's operational activities	1
Minor	Risks can hinder company activities but do not hinder the main activities of the company	2
Moderate	Risks hinder the course of business processes and result in the disruption of most company activities	3
Major	Risks cause obstacles to almost all company activities	4
Catastrophic	Risks cause all company activities to stop completely	5

After the likelihood and impact criteria of the risk are determined, the next step is to create an evaluation matrix. This evaluation matrix maps existing risks by dividing them into 5 levels, as shown in Tables 3 and 4.

Table 3. Evaluation matrix

Likelihood	*Certain*	**5**	**10**	**15**	**20**	**25**
	Likely	**4**	**8**	**12**	**16**	**20**
	Possible	**3**	**6**	**9**	**12**	**15**
	Unlikely	**2**	**4**	**6**	**8**	**10**
	Rare	**1**	**2**	**3**	**4**	**5**
Matriks Evaluasi		*Insignificant*	*Minor*	*Moderate*	*Major*	*Catastrophic*
		Impact				

Table 4. Risks by dividing into 5 levels

Risk Type	Deskripsi Risiko
Low Risk	Risks with little effect on the company can be addressed by implementing certain policies.
Medium Risk	Risks capable of causing slight disruptions in business can be addressed by implementing certain policies accompanied by supervision.
Medium-High Risk	Risks cause enough disruption that can be detrimental, so it requires supervision and handling.
High Risk	Dangerous and highly detrimental risks must be addressed as soon as possible.

4.2 Risk Assessment

4.2.1 Risk Identification

In assessing risk, it is necessary to know in advance what possible risks may occur that affect the company's activities and how much impact they have on the company's assets.

Table 5. Assessing risk

ID Risk	Risk	Impact
R01	Signal System Malfunction	Operational delays and potential collisions disrupt travel schedules, passenger confidence, and transportation assets.
R02	Sudden Power Outage	Train operations are disrupted and may even come to a halt
R03	Operational Errors by Operators	Potential accidents and rerouting errors
R04	Failure of Automatic Braking System	Potential collisions causing transportation asset losses and operational disruptions
R05	Failure of Passenger Evacuation Procedures	Emergency chaos may even result in passenger injuries and damage to the company's reputation.
R06	Flooding of Rail Areas	Delays or reductions in operating capacity and increased repair costs

ID Risk	Risk	Impact
R07	Physical Sabotage of Rails or Bridges	Damage to infrastructure causing major losses to physical assets and even passenger safety
R08	Corrosion of Rails or Support Structures	Potential malfunctions that require incidental maintenance and increased operating costs
R09	Non-compliance with Safety Protocols	Accidents due to technical or human error that may increase litigation risk
R10	Lack of Operational and Maintenance Funds	Service quality degradation and long-term performance degradation
R11	Ransomware Attacks on Operational Systems	Data is locked and service interrupted until a ransom is paid
R12	Denial-of-Service (DoS) Attacks	The central system loses response
R13	Eksploitasi Kerentanan pada SCADA	Train operational system control takeover
R14	Passenger Data Theft via IoT	Violation of passenger privacy may lead to decreased public trust and company reputation.
R15	Phishing of System Administrators	Sensitive systems and data may be altered and cause critical systems to break down.
R16	Insider Threats by IT Employees	Sabotage and alterations to systems that jeopardize operational integrity
R17	Insecure Integration of New Systems	New vulnerabilities exist that trigger the risk of exploitation of existing systems.
R18	Cloud Backup System Malfunction	Obstacles to service recovery due to data not being accessible when needed
R19	Attack on Supervisory Wireless Communication System	Wireless communications used to control trains are disrupted
R20	Man-in-the-Middle Attack on Communication Network	Attackers who infiltrate communications between trains and control centers can alter or steal data.
R21	Encryption System Failure on Passenger Data	Violation of privacy of users whose data is stolen because it is not properly encrypted

4.2.2 Risk Analysis

After the risks have been identified, the process continues by assessing the risks found based on the likelihood and impact values, as shown in Table 6.

Table 6. Risk Analysis

ID Risiko	Risiko	Likelihood	Impact	Total	Justifikasi
R01	Signal System Damage	2	5	10	Rarely due to routine maintenance and redundancy, the impact is very heavy due to safety.
R02	Sudden Power Outage	1	4	4	Very rare (dedicated power + backup), with heavy impact if it occurs.
R03	Operational Error by the Operator	2	4	8	Rarely, because of the strict training and SOPs, the impact is heavy.
R04	Automatic Braking System Failure	1	5	5	Very rare (multiple redundancy), the impact is very heavy.
R05	Failure of Passenger Evacuation Procedures	1	4	4	Very rarely due to routine drilling, heavy impact.
R06	Flooding in the Rail Area	1	3	3	Very rare (elevated track), moderate impact.
R07	Physical Sabotage on Rails or Bridges	1	5	5	Very rare (24/7 surveillance), the impact is very heavy.

ID Risiko	Risiko	Likelihood	Impact	Total	Justifikasi
R08	Corrosion on Rails or Support Structures	2	3	6	Rarely due to routine maintenance, the impact is moderate.
R09	Non-compliance with Safety Protocols	2	4	8	Rarely, because of training and monitoring, the impact is heavy.
R10	Lack of Operational and Maintenance Funds	2	3	6	Rarely (government backing), moderate impact.
R11	Ransomware Attacks on Operating Systems	2	4	8	Rarely, because of closed systems, the impact is heavy.
R12	Denial-of-Service (DoS) Attacks	1	3	3	Very rare (closed system), medium impact.
R13	Exploiting Vulnerabilities in SCADA	1	5	5	Very rare (air-gapped), the impact is very heavy.
R14	Passenger Data Theft via IoT	2	3	6	Rarely due to network segmentation, the impact is moderate.
R15	Phishing against System Administrators	3	4	12	Quite often, the impact is heavy.
R16	Insider Threats by IT Employees	1	5	5	Very rare (strict screening), the impact is very heavy.
R17	Unsafe New System Integration	2	4	8	Rarely, because of strict testing, the impact is heavy.
R18	Cloud Backup System Crashes	1	3	3	Very rare (multiple backups), medium impact.
R19	Attacks on Supervisory Wireless Communication Systems	2	4	8	Rarely because of encryption and monitoring, the impact is heavy.
R20	Man-in-the-Middle Attack on Communication Networks	2	4	8	Rarely because of end-to-end encryption, the impact is heavy.
R21	Encryption System Failure on Passenger Data	1	4	4	Very rare due to high standards and heavy impact.

Based on the risk analysis of the Indonesian LRT system, the majority of risks were at a low to medium level (score 3-8), with only two risks reaching a score ≥10. Phishing of system administrators was the highest risk, with a score of 12, followed by signal system malfunction, with a score of 10. This finding indicates that LRT Indonesia's infrastructure has implemented an effective risk management system, especially in terms of operational safety.

The analysis shows that risks with catastrophic impact (impact=5), such as automatic braking system failure and SCADA exploitation, are very unlikely due to the implementation of multiple redundancy systems and network isolation. Meanwhile, operational risks, such as power outages and flooding, show minimal likelihood, reflecting the effectiveness of the infrastructure design and backup systems installed.

4.2.3 Risk Evaluation

This is the last stage in assessing risk. At this stage, risk is mapped based on the risk value analyzed with a risk evaluation matrix. The results of the risk evaluation matrix can be seen in Table 7.

Table 7. Risk evaluation matrix

Likelihood	*Certain*	**5**	**10**	**15**	**20**	**25**
	Likely	**4**	**8**	**12**	**16**	**20**
	Possible	**3**	**6**	**9**	**12 (R15)**	**15**
	Unlikely	**2**	**4**	**6 (R08, R10, R14)**	**8 (R03, R09, R11, R17, R19, R20)**	**10 (R01)**
	Rare	**1**	**2**	**3 (R06, R12, R18)**	**4 (R02, R05, R21)**	**5 (R04, R07, R13, R16)**
Matrix Evaluation		*Insignificant*	*Minor*	*Moderate*	*Major*	*Catastrophic*
		Impact				

4.3 Risk Treatment

This stage connects risk identification with the implementation of effective strategies. It ensures that all stakeholders understand and can adjust the planned prevention and risk reduction measures according to their potential and impact.

Based on the analysis conducted in Table 8, the most significant risks in LRT Indonesia's operations are related to cybersecurity threats, particularly phishing attacks on system administrators (R15) and ransomware on operational systems (R11), which have a major impact on operational integrity and continuity.

Table 8. Risk identification with the implementation of effective strategies

ID Risiko	Risiko	Jenis Risiko	Rekomendasi Penanganan Risiko
R15	Phishing against System Administrators	12 (Medium High Risk)	Provide periodic training to administrators on phishing recognition and prevention. Ensure systems can only be accessed with additional authentication steps. Use an email filtering system to detect and block suspicious emails.
R01	Signal System Damage	10 (Medium-High Risk)	Improve signal system inspection schedules with IoT-based analytics. Ensure an automatic backup system is in place. Trained technicians to handle breakdowns quickly.
R03	Operational Error by the Operator	8 (Medium Risk)	Conduct regular training for operators on operational standards. Conduct emergency scenario simulations on a regular basis. Implement a real-time monitoring system to monitor operator activities.
R09	Non-compliance with Safety Protocols	8 (Medium Risk)	Conduct periodic audits to ensure compliance with safety protocols. Conduct socialization with all staff on the importance of safety protocols. Apply strict sanctions for protocol violations.
R11	Ransomware Attacks on Operating Systems	8 (Medium Risk)	Perform regular data backups in a separate location. Separate operational systems from public networks to perform network segmentation. Conduct regular security tests to detect vulnerabilities.
R17	Unsafe New System Integration	8 (Medium Risk)	Conduct a thorough security test before integrating a new system. Set strict operational standards for new system integration. Monitor the system after integration to detect anomalies.
R19	Attacks on Supervisory Wireless Communication Systems	8 (Medium Risk)	Use the latest encryption protocols, such as WPA3. Implement an IDS (Intrusion Detection System) system to monitor the communication network. Restrict network access to authorized devices only.

ID Risiko	Risiko	Jenis Risiko	Rekomendasi Penanganan Risiko
R20	Man-in-the-Middle Attack on Communication Networks	8 (Medium Risk)	Apply strong encryption to all data communications. Use a valid SSL/TLS certificate for connections. Monitor and analyze network traffic to detect suspicious activity.
R08	Corrosion on Rails or Support Structures	6 (Medium Risk)	Schedule periodic inspections of rails and supporting structures. Apply anti-corrosion coatings to extend the life of the materials. Monitor environmental factors such as humidity that can trigger corrosion.
R10	Lack of Operational and Maintenance Funds	6 (Medium Risk)	Optimize budget planning with a priority on operational essentials. Look for revenue alternatives such as advertising or sponsorship. Improve coordination with the government to ensure financial support.
R14	Passenger Data Theft via IoT	6 (Medium Risik)	Separate IoT devices from the main network. Use additional authentication technology for IoT access. Conduct periodic audits of connected IoT devices.
R04	Automatic Braking System Failure	5 (Medium Risk)	Implement an automatic backup braking system to improve reliability. Schedule component inspections and replacements. Periodically test the braking system through failure simulation.
R07	Exploiting Vulnerabilities in SCADA	5 (Medium Risk)	Separate the SCADA network from the public network to prevent unauthorized access. Use firewall and IDS technology to monitor access to the SCADA system. Update SCADA software regularly to cover vulnerabilities.
R13	Physical Sabotage on Rails or Bridges	5 (Medium Risk)	Increase surveillance around rail lines with CCTV technology and security patrols. Build security walls or fences to restrict access to vital lines. Increase cooperation with security forces to anticipate acts of sabotage.
R16	Insider Threats by IT Employees	5 (Medium Risk)	Conduct thorough background checks on potential employees. Ensure that no one individual has full control over critical systems. Implement a system to monitor suspicious employee activity on the system.
R02	Sudden Power Outage	4 (Low Risk)	Ensure the system has an Uninterruptible Power Supply (UPS) to maintain operational continuity. Ensure backup generators are always ready for use. Actively coordinate with electricity providers to reduce the risk of outages.
R05	Failure of Passenger Evacuation Procedures	4 (Low Risk)	Conduct periodic evacuation simulations to ensure procedures are running well. Ensure warning systems in all cars and stations are functioning optimally. Ensure all staff understand their respective roles in an evacuation scenario.
R06	Flooding in the Rail Area	3 (Low Risk)	Improve the quality of the drainage system around the rail area. Monitor the condition of rail lines especially in the rainy season. Prepare quick procedures for evacuation and dewatering of flooded tracks.
R12	Denial-of-Service (DoS) Attacks	3 (Low Risk)	Use firewall software that can detect and block DoS attacks. Monitor network traffic to detect suspicious volume increases. Set up backup servers to ensure operations continue.
R18	Cloud Backup System Crashes	3 (Low Risk)	Use multiple cloud backup providers to ensure data remains secure. Automatically monitor backup performance. Perform regular data recovery tests to ensure backup integrity.

Meanwhile, technical risks such as signal system malfunction (R01) and automatic braking system failure (R04) also show severe impacts that can threaten passenger safety. Effective risk management includes improvements in training, enhancing redundancy systems, strengthening supervision, and developing more resilient backup infrastructure. Strict implementation of security protocols, regular system testing, and improved management of operational budgets and funds also need to be optimized to mitigate the impact of lesser risks such as flooding or sudden power outages.

5. Discussion

This research aims to identify threats and provide solutions to security challenges in Light Rail Transit (LRT) systems in Indonesia. Using the ISO-31000:2018 framework approach, this research offers a structured method to evaluate and mitigate the risks faced. One of the main GAPs is the lack of research that specifically addresses LRT system security by considering Indonesia's local characteristics, such as transportation infrastructure, geographical conditions, and applicable policies. Most previous studies, such as "Transportation Security: Potential Threats and Strategies to Deal with Them," discuss public transportation security in general without highlighting the specifics of transportation modes such as LRT (Ulil, 2020). This study differs in that it tailors threats and solutions to the unique conditions faced by Indonesian LRT, including the threats of flooding, physical sabotage, and IoT-based cyberattacks.
In addition, this research has advantages over research that focuses on cyber threats. This research takes a broader approach by combining operational, technical, and cyber threats in one evaluation framework. The use of the ISO-31000:2018 framework enables a structured analysis, including risk assessment based on likelihood and impact and more systematic mitigation recommendations. In this regard, this study offers a comprehensive view that covers all aspects of LRT security, from the risk of signaling system malfunction to ransomware threats.

Another distinguishing feature is the emphasis on practical technology- and management-based recommendations that can be implemented directly by LRT managers. For example, the study suggests the integration of IoT technology to improve signal inspection and the use of WPA3 encryption protocol to prevent cyberattacks. This approach is more applicable compared to previous studies that only discussed the implementation of certain technologies without linking them to a thorough risk evaluation. With this comprehensive approach, this research makes a significant contribution to the study of public transportation security in Indonesia. In addition, it also offers a solid foundation for the implementation of innovative, relevant and sustainable security solutions. Therefore, this research not only closes the GAP in the literature but also provides practical added value for LRT managers and other stakeholders.

6. Conclusion

This research analyzes the security threats and solutions to the Light Rail Transit (LRT) system in Indonesia using the ISO-31000:2018 approach, which provides a structured framework for risk identification and mitigation. Based on the study's results, the majority of threats are at low to medium risk levels, with the highest threats involving phishing attacks and signal system malfunctions. The findings reveal the effectiveness of the risk management system that has been implemented, although there is still room for improvement, especially in the management of cyber threats.
This research is unique in combining operational, technical and cyber perspectives into a comprehensive evaluation framework. Compared to previous research, such as studies that only focus on the implementation of certain technologies or general risk analysis, this research offers insights specific to the Indonesian context. For example, the integration of IoT and AI-based technologies for early detection and threat mitigation shows a more innovative and applicable approach. As such, this research not only fills a gap in the literature related to LRT security but also provides practical recommendations that are relevant and directly applicable to LRT managers in Indonesia. The findings provide an important basis for building a safer and more reliable public transportation system.

Recommendation

Based on the findings of this study, it is recommended that the Indonesian LRT management do the following: 1). Conduct periodic training on cybersecurity for all staff, especially those responsible for

system administration. 2). Increase the frequency of inspection and maintenance of signal systems with IoT technology for early detection of problems. 3). Implement a multi-factor authentication system to reduce the risk of phishing. 4). Establish collaboration with law enforcement and cybersecurity service providers for rapid response to threats. 5). Conduct regular emergency simulations to ensure preparedness for various risk scenarios.

References

Firmansyah, M., & Yuswanto, A. (2022). Manajemen Pengetahuan Penanganan Insiden Keamanan Informasi Pada Security Operation Centerdi Pemerintah Provinsidki Jakarta. Jurnal Inovasi Aparatur, 4(2), 441-452.

Hakim, L. (2024). *Manajemen Transportasi dan Akomodasi Pariwisata*. Deepublish.

Kharisma, L. P. I., Kelvin, K., Sudiro, S. A., Suprianto, G., Judijanto, L., Lutfi, M., ... & Yuniansyah, Y. (2024). Internet of Things: Pengenalan dan Penerapan Teknologi IoT. PT. Sonpedia Publishing Indonesia.

Kemmala, D., & Aris, K. (2023). Pengembangan Sistem Transportasi Masa Depan: Mobilitas Berkelanjutan dan Otonom di Jawa Barat. Jurnal Multidisiplin West Science, 2(9).

Margaretha, T. N. (2023). *Evaluasi Kinerja Pelayanan Light Rail Transit di Kota Palembang* (Doctoral dissertation, Universitas Islam Indonesia).

Matsika, E., O'Neill, C., Battista, U., Khosravi, M., Laporte, A. D. S., & Munoz, E. (2016). Development of Risk Assessment Specifications for Analysing Terrorist Attacks Vulnerability on Metro and Light Rail Systems. *Transportation Research Procedia*, *14*, 1345–1354. https://doi.org/10.1016/j.trpro.2016.05.207

Purwani, F., Zakia, A. M. A., Irillah, M. I., & Intaniansyah, F. (2024). Implementasi Metode Prototype Pada Perancangan Sistem Informasi Web: Solusi Meningkatkan Pelayanan Dan Efisiensi Lrt Di Kota Palembang. *Jurnal Riset Teknik Komputer*, *1*(4), 08-15.

Putri, N. H. A., & Sahara, S. (2023). Analisis penambahan sarana penunjang kegiatan LRT untuk kemudahan mobilitas masyarakat di wilayah Palembang. Advances In Social Humanities Research, 1(12), 31-37.

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). Jurnal Pengabdian Nasional (JPN) Indonesia, 6(1), 38-52.

Sarjito, I. A., Duarte, E. P., & Sos, S. (2023). Geopolitik dan Geostrategi Pertahanan: Tantangan Keamanan Global. Indonesia Emas Group.

Sianturi, R. R., Harahap, M. A. K., & Saragih, H. (2025). Perencanaan Tata Ruang Kota untuk Mendukung Mobilitas Berkelanjutan. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, *4*(2), 2324-2332.

Soleh, M., & Tjenreng, Z. (2025). Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital. Jurnal Kajian Pemerintah: Journal of Government, Social and Politics, 11(1), 1-10.