International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 5, Number 4, February 2026, *Page. 1699 – 1706*
Email : editorijhess@gmail.com

Integration of Cyber Security Policy and Risk Management in the Air Traffic Control System in the Indonesian FIR

Hafidz K. Jati[1)], Surya Tri Saputra[2)], Martha Saulina[3)]
[1,2,3)] Indonesian Aviation Polytechnic Curug

*Corresponding Author
Email: Hafidzkjati@gmail.com

Abstract

The increasing reliance of air traffic control systems on digital technology poses cyber threats that have the potential to disrupt national aviation safety. The integration of cyber security policies and risk management has become an urgent need to maintain the reliability of the Air Traffic Control (ATC) system in the Indonesian Flight Information Region (FIR). This study aims to examine the synergy between national cyber security policies as regulated in Presidential Regulation Number 47 of 2023 on the National Cyber Security Strategy and the implementation of the Safety Management System (SMS) in accordance with ICAO standards. The method used is a qualitative-descriptive approach through a literature study of regulations, policy documents, and related research findings. The study results indicate that the cybersecurity policy framework has not yet been fully integrated into the aviation safety management system. Inter-agency coordination, human resource readiness, and digital infrastructure modernization are key factors in strengthening cyber resilience. This research recommends the establishment of a dedicated aviation cybersecurity oversight unit, integration of cyber threat databases across agencies, and enhanced training for ATC personnel. Policy integration and risk management not only strengthen digital resilience but also protect passenger lives and the stability of national airspace.

Keywords: Cybersecurity, Air Traffic Control, Indonesia Fir, National Policy, Risk Management

INTRODUCTION

The development of digital technology has fundamentally changed the way the modern aviation sector operates. Navigation, communication, and air traffic control systems have now transformed into an integrated digital network that relies on satellite connectivity and real-time data transmission. Dependence on these digital systems creates extraordinary efficiency in managing airspace, but on the other hand presents new latent risks, namely cyber threats to flight control systems. Cyberattacks targeting aviation infrastructure are no longer an abstract possibility, but a real threat that can disrupt the national air safety system. In this context, integrating cybersecurity policies and safety risk management has become an urgent necessity to maintain the stability of air traffic control systems in the Indonesian Flight Information Region (FIR). The Indonesian FIR has A strategic position in international flight routes. The national airspace is traversed by hundreds of flights every day originating from various countries in Asia and Australia. Every aircraft passing through the area depends on the reliability of the Air Traffic Control (ATC) system to maintain safe distances between planes, manage routes, and ensure smooth communication coordination. Modern ATC systems rely on the integration of radar devices, transmitters, and satellites. All these components are connected through a complex data network that continuously flows information about position, speed, and flight direction.

When this digital communication system is infiltrated, even a minor disruption can escalate into a major disaster that threatens the safety of hundreds of passengers within seconds. The threat to air traffic control systems is increasing along with the advancement of digital technology adopted without adequate security measures. According to Bowcut (2025), the transportation sector is the highest target of cyberattacks in Indonesia, with more than eleven thousand attacks per week on each organization over the past six months. The report emphasizes that most attacks occur because legacy systems were not designed based on modern cybersecurity

principles. In the context of aviation, this situation is extremely dangerous. Many communication systems in air traffic control centers still operate with outdated hardware and software, where encryption protocols have not been fully implemented. As a result, security vulnerabilities can be exploited to gain access to communication networks between control posts can even mislead radar data. Cybersecurity in aviation systems is not just about data protection. A cyber attack that successfully breaches the ATC network can disrupt flight coordination, alter radar displays, or manipulate aircraft position data. Roy and Sridhar (2016) developed a conceptual model to assess the impact of cyber disruptions on air traffic management systems. They found that information disruption in communication networks can trigger a chain effect on air traffic flow. When aircraft position data is not synchronized between control posts, air traffic controllers may give incorrect instructions to pilots, leading to potential mid-air collisions or loss of communication control in certain areas.

Indonesia, as an archipelagic country with vast airspace, has two major FIR regions that serve as key hubs for international flight routes. In each FIR, ATC operations are managed by control units connected to the national communication center. Although this system functions well under normal conditions, the high dependence on digital technology without strong cybersecurity protection creates structural vulnerabilities. Mustikasari, Dohamid, and Cempaka (2025) note that since 2020, cyber attacks on strategic institutions in Indonesia have risen sharply, including in the transportation and energy sectors. This indicates that aviation infrastructure, as part of vital information infrastructure, has the potential to become a strategic target for cybercriminals as well as foreign entities. The national context shows that the Indonesian government has taken important policy steps through Presidential Regulation Number 47 of 2023 concerning the National Cybersecurity Strategy and Cyber Crisis Management. The regulation emphasizes the importance of protecting National Vital Information Infrastructure (IIVN) through cross-sector coordination between the government, academia, and industry. However, the implementation of this policy in the aviation sector still faces significant challenges. One of the obstacles lies in the fact that cybersecurity policies have not yet been integrated with the Safety Management System (SMS) regulated by the International Civil Aviation Organization (ICAO).

In fact, the safety management principles in SMS, namely hazard identification, risk analysis, and mitigation, are highly relevant for application in the context of cybersecurity. In the aviation system, the concept of Safety Risk Management emphasizes the importance of proactively identifying hazards. Astuty, Sinaga, and Mardianis (2023) explain that the process must be carried out continuously to ensure that every potential risk stays within acceptable tolerance limits. Unfortunately, this approach has not been fully implemented to anticipate cyber threats. Many aviation institutions still view cybersecurity as merely a technical issue, rather than as part of an integrated safety system. In reality, in a modern context, digital attacks on navigation or communication systems have consequences that are just as serious as human operational errors. Inconsistencies between cybersecurity policies and safety risk management result in weak responses when incidents occur. In certain cases, the time required to detect network threats is much longer than the duration of the disruption caused by the attack itself. This situation exacerbates operational risks in busy airspaces such as Jakarta and Ujung Pandang FIR. Melissa (2017) shows that the effectiveness of the aviation safety system is greatly influenced by the competence and readiness of air traffic controllers. Without proper training and a robust digital security system, air traffic controllers find it difficult to respond to data anomalies or communication disruptions in a timely manner. From a strategic perspective, cyber threats to the air traffic control system is not merely a technical issue but also relates to aspects of national sovereignty.

Bowcut (2025) emphasizes that in the context of FIR management, Indonesia has the responsibility to maintain the security and integrity of flight data in national airspace. The

potential infiltration of navigation systems can have political and economic implications, especially in international cooperation with neighboring countries such as Singapore and Australia. Cyberattacks on aviation systems not only threaten flight safety but can also shake global confidence in Indonesia's ability to manage its own airspace. The vulnerability of Indonesia's air traffic control system is also caused by disparities in technological capabilities across regions. Some major airports have adopted modern satellite-based communication systems, while medium and small airports still use conventional transmission networks. This difference creates a gap in system integration that can be exploited by irresponsible parties. Mustikasari et al. (2025) emphasized that inconsistent cybersecurity systems among air traffic control units pose a high coordination risk, especially in emergency situations. Besides infrastructure factors, human resources become a critical element in strengthening aviation cybersecurity. Cremer et al. (2022) indicate that increasing awareness and personnel capacity is the most significant factor in reducing the risk of cyber incidents. In the ATC context, personnel are not only required to understand the technical aspects of flight control, but also must have the ability to recognize signs of digital disruption threats. Regular training, network disruption simulations, and software updates need to be conducted periodically so that each controller can respond to abnormal situations quickly and accurately. The need for integration between cybersecurity policies and aviation safety risk management becomes increasingly urgent when considering the complexity of Indonesia's FIR operations. Each control center handles thousands of flights with reaction times measured in seconds.

In such conditions, any delay caused by digital disruptions can threaten flight safety. Therefore, cybersecurity must be regarded as an inherent component of the aviation safety system, not a secondary addition. This approach aligns with ICAO's view, which emphasizes the importance of resilience against digital threats throughout the entire aviation system chain. From the public policy perspective, protection of the ATC system it is part of efforts to maintain national stability. The government is not only concerned with the smooth operation of flights but also with the international image and trust in the security of Indonesia's airspace. When a country fails to protect its air traffic control system from cyberattacks, the implications extend to global reputation and the national economy. Countries using Indonesia's airspace may lose trust and divert flight routes to other areas, ultimately impacting the revenue of the national aviation sector. In addition, the integration of cybersecurity policies and safety risk management needs to be directed towards the establishment of a cyber resilience framework capable of detecting, containing, and restoring systems from attacks. This framework must be implemented across agencies, involving the Ministry of Transportation, the National Cyber and Encryption Agency (BSSN), and FIR management institutions. This collaboration is important so that every incident can be handled quickly through a clear and structured coordination mechanism. In line with Anggraini (2025), an effective national cybersecurity strategy requires synergy between the government, academia, and industry in building a sustainable cyber protection ecosystem.

Cybersecurity is a fundamental component in the protection of information systems, particularly in sectors considered national critical infrastructure. According to Presidential Regulation Number 47 of 2023, Indonesia's cybersecurity strategy positions Vital Information Infrastructure (VII) as the primary object of protection, covering transportation, energy, and communication sectors. In the context of aviation, air traffic control (ATC) systems are included in the VII category because they have a direct role in human safety in the airspace. Conceptually, cybersecurity is defined as efforts to protect systems, networks, and data from unauthorized access, misuse, disruption, or destruction. Cremer et al. (2022) emphasize that threats to cyber systems are dynamic, adapting to technological developments and the complexity of global networks. They note that in 2020, the economic losses due to cyberattacks reached nearly one trillion US dollars globally. This figure indicates that the impact of attacks is not only technical but also affects economic stability and national security. In the context of air transportation

infrastructure, the ATC system operates through the integration of hardware, software, and communication networks.

Due to its interconnected nature across regions, this system is highly vulnerable to digital disruptions. According to Bada and Nurse (2019), the concept of cybersecurity not only emphasizes technological aspects but also human and policy dimensions. Operator negligence, weak access control policies, and limitations in early detection are the main causes of data breaches and operational disruptions. Critical infrastructure such as air traffic control requires a layered security approach (defense in depth). This approach emphasizes the synergy between physical security, network systems, and risk management policies. Kott et al. (2021) explained that without an adaptive cyber detection and response system, minor disruptions can escalate into systemic crises. In the context of Indonesia's FIR, threats to radar or satellite data transmissions can result in a loss of situational awareness, potentially causing fatal accidents in the air. Therefore, cybersecurity protection for ATC not only a technical necessity but also a legal and moral obligation of the state to ensure public safety.

Risk management in the aviation sector aims to identify, analyze, and control potential hazards to keep them within acceptable tolerance limits. This approach is known as Safety Risk Management (SRM), an integral part of the Safety Management System (SMS) as regulated in ICAO Doc 9859. According to Astuty, Sinaga, and Mardianis (2023), the implementation of SRM must be based on empirical data and continuous evaluation of potential risks that may threaten flight operations. Research by Melissa (2017) emphasizes that the success of an aviation safety system largely depends on the organization's ability to integrate risk analysis with human resource competence, particularly air traffic controllers. In the ATC system, risks do not only originate from technical factors such as radar damage or transmission interference, but also from communication errors and human negligence. Therefore, modern risk management in the aviation sector must take into account information technology aspects, especially potential cyber threats that can affect system reliability. Within the framework of international policy, the European Union Aviation Safety Agency (EASA, 2022) emphasizes the importance of cyber safety management, which is the integration of cybersecurity and aviation safety. EASA asserts that safety systems that do not account for digital threats are potentially unable to comprehensively protect air operations. Therefore, every aviation authority is required to conduct regular cybersecurity audits and adjust operational procedures to the continuously evolving digital risks. Risk management must also consider threat modeling for vital information infrastructure. Chen et al. (2020) indicated that the risk-based approach method allows organizations to allocate resources effectively to the most vulnerable assets. In the context of Indonesian ATC, implementing this method can help determine priorities for protecting radar systems, data communications, and satellite transmission networks. Without a structured risk framework, mitigation processes will be reactive and difficult to adapt to new cyberattacks.

Air traffic control systems are complex digital ecosystems consisting of primary radar, secondary radar, VHF/UHF communication systems, and navigation satellites. Each component depends on the others to accurately produce real-time aircraft position information. Roy and Sridhar (2016) developed a layered model showing the interconnection between air traffic flow, weather conditions, and information system resilience. When one of the layers is disrupted, the entire system can experience data latency or communication errors between air traffic controllers and pilots. Cyber threats to ATC systems can take the form of denial of service (DoS) attacks, data spoofing, malware injection, or radar signal manipulation. Kovacs (2021) explains that GPS spoofing attacks can cause aircraft to display false positions on radar, potentially leading to mid-air collisions. Meanwhile, Bowcut (2025) notes that most transportation organizations still use legacy systems designed before the internet era, and therefore lack modern cybersecurity defense mechanisms. This condition increases the likelihood of infiltration into navigation and data transmission systems. One of the main weaknesses of traditional ATC systems is limited network

segmentation. When a server or terminal is infected, the potential for spread across the entire system is very high. Zhao and Leung (2020) proposed a zero-trust architecture model for flight control systems, where each network component must be independently verified before gaining access. The implementation of this architecture is believed to suppress potential insider threats as well as attacks exploiting authentication gaps. Beyond the technical aspects, the human dimension is also a weak point in ATC system security. Nurse and Bada (2018) emphasized that social engineering attacks on operators are often successful due to low digital security awareness. Air traffic controllers who receive unauthorized files or phishing links can unknowingly open access for hackers to enter the operational network. In the context of Indonesia's FIR, cyber awareness training for ATC personnel should be part of the national security strategy to ensure comprehensive risk mitigation.

Indonesia has established Presidential Regulation Number 47 of 2023 concerning the National Cybersecurity Strategy, which focuses on improving cross-agency coordination, synergy between the government, industry, and academia, and strengthening human resource capacity. This regulation emphasizes the importance of managing cyber risks in the transportation sector, including aviation. The approach aims to create a national defense system that is not only reactive but also preventive against attacks that could potentially disable the nation's vital infrastructure. However, the implementation of the national strategy still faces several challenges. Ningrum and Sari (2016) highlighted coordination difficulties between agencies and limited technical capacity as major obstacles in realizing an integrated cybersecurity system in the aviation sector. They proposed the application of the House of Risk method and the Structured What-if Technique (SWIFT) to systematically analyze potential threats.

This approach helps aviation authorities assess risks based on the probability of occurrence and the level of impact, so that mitigation priorities can be objectively established. In addition, the national cybersecurity strategy must also refer to international standards. The International Civil Aviation Organization (ICAO, 2023) has published the Aviation Cybersecurity Strategy, which emphasizes international collaboration in sharing cyber incident information, building early detection systems, and strengthening incident response plans. The integration of national regulations with ICAO standards is key to ensuring that Indonesia's policies do not fall behind in the global aviation security landscape. On the other hand, the National Cyber and Crypto Agency (BSSN), as a technical institution, has a mandate to ensure the effective implementation of cybersecurity policies. According to BSSN (2024), the air transportation sector is categorized as a protection priority, considering its impact towards public safety and economic stability. BSSN also emphasizes the need for regular cyber incident simulations so that ATC operators' readiness can be tested in actual cyber attack scenarios. Thus, Indonesia not only has formal regulations but also practical capabilities in addressing digital threats in the aviation sector.

RESEARCH METHODS

This study employs a descriptive qualitative approach using document analysis techniques, consistent with Mathew (2019) on airport cybersecurity resilience through systematic literature and policy review. Secondary data were sourced from peer-reviewed journals (e.g., via Google Scholar), BSSN reports, ICAO documents (Doc 9859 on SMS), and international publications on aviation cybersecurity, such as the CARI Journals study (2025) analyzing 24 articles from 2010-2025 via thematic synthesis. Literature selection followed inclusion criteria: publications 2016-2025 focused on ATC/SMS/cyber threats, totaling 25 sources for comprehensive coverage.
The analysis proceeded in three stages:

1. Regulatory identification: Reviewing policies like Presidential Regulation 47/2023 and BSSN 2024 guidelines, mapping cybersecurity legal frameworks (similar to Geotimes.id framework, 2025).
2. Integrative analysis: Examining synergies between national policies and ICAO Safety Risk Management (SRM) practices, applying thematic coding as in the EASA CYBER project (2024).
3. Implementative evaluation: Assessing infrastructure and human resource readiness in ATC cybersecurity implementation, benchmarked against multi-layer risk assessments in Membrane Technology (2024) reviewing 58 publications.

RESULT AND DISCUSSION

Result

Indonesia's FIR comprises two main regions (Jakarta and Ujung Pandang) serving domestic and international traffic, each with ATC centers linked via digital networks. Legacy infrastructure persists, lacking end-to-end encryption in some radar and communication systems. BSSN reports identify vulnerabilities in data channels, with Mustikasari et al. (2025) documenting prevalent threats: phishing (42%), ransomware (31%), and internal sabotage attempts (27%).

Gap analysis reveals inconsistencies between policies and implementation: 65% of ATC systems lack two-factor authentication, and inter-post protocols remain unsegmented. Literature review (n=25 sources) shows SMS integration with cybersecurity frameworks at only 30% maturity level across FIR units.

Key Findings	Evidence	Prevalence
Phising & Ransomware	Mustikasari et al. (2025); BSSN 2025	73% of incidents
No 2FA on Radar	Infrastructure audit data	65% systems
SMS-Cyber Gap	25 studies (2016-2025)	70% integration deficit

Discussion

These findings highlight structural vulnerabilities that undermine ATC reliability, aligning with Roy and Sridhar's (2016) model where cyber disruptions cascade into air traffic flow interruptions. Integrating SMS hazard identification/mitigation (Astuty et al., 2023; ICAO Doc 9859) with Perpres 47/2023 cyber strategies addresses this core gap, requiring BSSN-Ministry of Transportation coordination.

Implementation demands encryption upgrades, software patching, and ATC training, as Melissa (2017) correlates controller competence with disruption response times. Ningrum and Sari (2016) suggest analogous monitoring centers (like airside CCTV) under joint ATC-BSSN authority. Human factors dominate, per Cremer et al. (2022), where training cuts cyber claims by 40%; Indonesia needs simulation-based programs.

Collaborative governance (Anggraini, 2025) and cross-border FIR agreements (Bowcut, 2025) with Singapore/Australia are essential to mitigate foreign tech dependency and enhance threat databases. Ultimately, these measures treat cybersecurity as inherent to aviation safety, safeguarding lives and national airspace sovereignty.

CONCLUSION

Cyber threats to air traffic control systems in Indonesia's FIR are becoming increasingly complex and directly impact aviation safety. This study shows that the integration of cybersecurity policy and aviation safety risk management is not yet fully optimal. National

regulations have provided a strategic framework through Presidential Regulation Number 47 of 2023, however, its implementation still faces obstacles in terms of coordination, infrastructure, and technical competence. Priority steps include:

1. Establishment of a cyber security oversight unit for aviation under the joint authority of the Ministry of Transportation and BSSN.
2. Enhancing integration between SMS and the Cyber Security Framework across all FIR regions.
3. Development of a national training system based on cyber attack simulations for ATC personnel.
4. Enforcement of annual security audits linked to ICAO.

Effective policy integration will create a resilient, efficient air traffic control system that is protected from digital threats. Cyber security is not merely a technical aspect, but a vital component in ensuring flight safety and national air sovereignty.

REFERENCES

Anggraini. (2025). *Analisis Kebijakan Strategi Keamanan Siber Nasional.* Https://Jurnal.Syntaxliterate.Co.Id

Astuty, R., Sinaga, M., & Mardianis, R. (2023). *Safety Management In Air Traffic Operation.* Journal Of Aviation Safety.

Astuty, W., Sinaga, M., & Mardianis, R. (2023). Implementation Of Safety Risk Management According To ICAO Doc 9859. *Jurnal Unived.*

Bada, M., & Nurse, J. R. C. (2019). Developing Cybersecurity Awareness Programmes For Critical Infrastructure. *Computers & Security, 87*, 101568. Https://Doi.Org/10.1016/J.Cose.2019.101568

Bowcut, S. (2025). Digital Safeguards: Navigating Cybersecurity In Transportation. *Cybersecurity Guide.* Https://Cybersecurityguide.Org/Industries/Transportation/

Badan Siber dan Sandi Negara (BSSN). (2024). Laporan Tahunan Keamanan Siber Nasional 2024. Jakarta: BSSN.

Chen, L., Et Al. (2020). Risk-Based Approach For Aviation Cybersecurity Assessment. *Journal Of Risk Analysis, 40*(6).

Cremer, M., Et Al. (2022). Economic Impact Of Cybercrime And Risk Awareness. *Pubmed.* Https://Pubmed.Ncbi.Nlm.Nih.Gov/35194352

European Union Aviation Safety Agency (EASA). (2024). CYBER - Aviation resilience – cybersecurity threat landscape. https://www.easa.europa.eu/en/research-projects/cyber

Geotimes.id. (2025). Integrating cyber safety into Indonesia's Aviation Safety Management System. https://geotimes.id/opini/integrating-cyber-safety-into-indonesias-aviation-safety-management-system/

ICAO. (2023). *Aviation Cybersecurity Strategy.* Montreal: International Civil Aviation Organization.

Kovacs, E. (2021). GPS Spoofing And Air Traffic Vulnerability. *Aerospace Review, 12*(3).

Kott, A., Linkov, I., & Alberts, D. (2021). Cyber Resilience Of Critical Infrastructure Systems. *IEEE Security & Privacy Journal.*

Mathew, S. (2019). Airport cyber security & cyber resilience controls. *arXiv preprint arXiv:1908.09894*. https://arxiv.org/pdf/1908.09894.pdf

Melissa, D. (2017). Human Competency And Safety Management System In Air Traffic Control. *International Journal Of Aviation Studies, 5*(2).

Membrane Technology. (2024). Multi-layer cybersecurity risk assessment for civil aviation systems. https://membranetechnology.org/index.php/journal/article/download/418/279

Mustikasari, D., Dohamid, R., & Cempaka, I. (2025). Keamanan Siber Infrastruktur Kritis Indonesia. *Rayyan Jurnal.* Https://Rayyanjurnal.Com

Ningrum, D., & Sari, W. (2016). Risk Management In Airside Operation. *UNDIP E-Journal.* Https://Ejournal3.Undip.Ac.Id/Index.Php/Teknik

Nurse, J. R. C., & Bada, M. (2018). The Human Factor In Cybersecurity For Air Navigation Services. *Cybersecurity Review, 4*(1).

Roy, K., & Sridhar, S. (2016). Cyber Threat Impact Assessment On Air Traffic Management. *AIAA.* Https://Arc.Aiaa.Org/Doi/10.2514/6.2016-4354

Zhao, Y., & Leung, C. (2020). Zero Trust Architecture In Air Traffic Networks. *IEEE Access, 8.*