Towards a Resilience Framework for Securing ADS-B Surveillance Systems in Air Traffic Management

Victoria Mofolo
VLM Aviation Infrastructure Advisory / Regenesys Business School, South Africa

mofolovictoria2@gmail.com

Abstract: Automatic Dependent Surveillance–Broadcast (ADS-B) has become a cornerstone of modern air traffic surveillance, enabling real-time aircraft tracking and supporting enhanced situational awareness within Air Traffic Management (ATM) systems. However, the open and unauthenticated nature of ADS-B transmissions introduces significant cybersecurity vulnerabilities, including spoofing, jamming, and data injection attacks. These threats pose risks not only to surveillance integrity but also to operational trust and decision-making in safety-critical environments. This paper presents a resilience-based cybersecurity framework for securing ADS-B systems within ATM environments, with particular consideration of resource-constrained and evolving airspace environments. The proposed framework integrates technical detection mechanisms, operational response strategies, and governance principles to enhance system robustness against cyber-physical threats. A scenario-based approach is adopted to illustrate how the framework supports the detection and management of anomalous ADS-B behaviour, while maintaining continuity of surveillance services. The contribution of this work lies in bridging the gap between theoretical vulnerability analysis and practical resilience design in aviation surveillance systems. The framework provides a structured foundation for enhancing cybersecurity posture in ADS-B-enabled environments and supports ongoing research into resilient and trustworthy air traffic systems.

Keywords: ADS-B, Aviation cybersecurity, Air traffic management, Resilience, Surveillance systems, Decision-making

1. Introduction

The increasing reliance on digital surveillance technologies has fundamentally reshaped the operational landscape of Air Traffic Management (ATM). Among these technologies, Automatic Dependent Surveillance–Broadcast (ADS-B) has emerged as a critical enabler of real-time aircraft tracking, supporting enhanced situational awareness, improved airspace efficiency, and the transition toward data-driven air traffic operations. By broadcasting aircraft position, velocity, and identification data, ADS-B enables more dynamic and responsive decision-making within increasingly complex airspace environments.

However, despite its operational advantages, ADS-B was not designed with security as a foundational requirement. The system's open and unauthenticated broadcast architecture introduces inherent vulnerabilities, including spoofing, jamming, and message injection attacks. These vulnerabilities are no longer theoretical; they represent a growing class of cyber-physical risks capable of compromising surveillance integrity and, more critically, undermining trust in the data upon which operational decisions are made.

This shift introduces a fundamental challenge for modern ATM systems. Surveillance is no longer simply about data availability, but about **data trustworthiness under contested conditions**. In safety-critical environments, where decisions must be made in real time, the presence of unreliable or manipulated surveillance data can have cascading operational consequences, including degraded situational awareness, incorrect controller actions, and reduced safety margins.

While existing research has extensively examined the technical vulnerabilities of ADS-B systems, much of this work remains focused on isolated attack scenarios or detection mechanisms. Less attention has been given to how these vulnerabilities translate into operational risk, and how ATM systems can maintain continuity, stability, and trusted decision-making in the presence of cyber threats. This gap highlights the need for a broader perspective that moves beyond vulnerability identification toward system-level resilience.

This paper addresses this gap by proposing a resilience-oriented cybersecurity framework for ADS-B surveillance systems within ATM environments. The framework integrates technical detection mechanisms, operational response strategies, and governance considerations to support the maintenance of surveillance integrity and continuity under adverse conditions. A scenario-based approach is used to illustrate how ADS-B anomalies can be detected, interpreted, and managed within real-world operational contexts.

The contribution of this work lies in reframing ADS-B cybersecurity as a **systemic resilience challenge**, rather than a purely technical problem. By linking vulnerabilities to operational decision-making and governance structures, the proposed framework provides a structured foundation for enhancing trust, robustness, and adaptability in next-generation air traffic surveillance systems.

2. Background and Literature Review

The evolution of surveillance technologies in aviation has been driven by the need for improved situational awareness, increased airspace capacity, and enhanced operational efficiency. Traditional radar-based systems, including Primary Surveillance Radar (PSR) and Secondary Surveillance Radar (SSR), have historically formed the backbone of air traffic surveillance. However, these systems are associated with high infrastructure and maintenance costs, as well as limitations in coverage, particularly in remote or oceanic airspace.

The introduction of Automatic Dependent Surveillance–Broadcast (ADS-B) represents a significant shift towards cooperative and satellite-enabled surveillance, enabling more precise and cost-effective tracking of aircraft. ADS-B operates by broadcasting aircraft-derived data, including position, velocity, and identification, to ground stations and other aircraft, supporting real-time tracking and advanced Air Traffic Management (ATM) concepts such as trajectory-based operations.

Despite these advantages, ADS-B was designed with a focus on interoperability and efficiency rather than security. As a result, transmissions are neither encrypted nor authenticated, making them inherently vulnerable to cyber threats. Existing literature has demonstrated the feasibility of spoofing attacks, jamming, and message injection (Costin and Francillon, 2012; Strohmeier et al., 2015), all of which can compromise surveillance accuracy and mislead operational decision-making.

While these studies provide valuable insights into technical vulnerabilities, they often focus on isolated attack scenarios. More recent research has explored mitigation strategies such as multilateration, cryptographic enhancements, and anomaly detection (Leonardi et al., 2017; Illiashenko et al., 2023). However, practical implementation remains constrained by interoperability requirements, legacy systems, and regulatory limitations, particularly in resource-constrained environments.

3. Research Problem and Gap

Despite extensive research into ADS-B vulnerabilities and mitigation techniques, a critical gap remains in understanding how these vulnerabilities impact operational decision-making within real-world ATM environments. Existing approaches primarily focus on detection and prevention at a technical level (Dave et al., 2022; Ukwandu et al., 2022), with limited integration of operational and governance considerations.

In practice, air traffic systems must continue to function under conditions of uncertainty, degraded data integrity, and potential cyber interference. The challenge is therefore not only to detect anomalies, but to ensure that operational decisions remain safe, reliable, and informed even when surveillance data cannot be fully trusted.

This highlights a fundamental shift from a vulnerability-centric perspective to a resilience-oriented perspective, where the focus extends beyond preventing attacks to maintaining continuity of operations and trust in decision-making processes.

4. Research Methodology

This study adopts a qualitative, scenario-based research approach, supported by a structured review of existing literature (Illiashenko et al., 2023) on ADS-B vulnerabilities and mitigation strategies.

Three representative cyber threat scenarios are considered:

- ADS-B spoofing (injection of false aircraft data)
- Trajectory manipulation (alteration of aircraft movement patterns)
- Signal degradation or jamming

These scenarios are used to analyse the impact of cyber threats on surveillance integrity and operational decision-making.

In addition, preliminary practitioner insights are incorporated through survey-based input from aviation and cybersecurity professionals. While not statistically representative, these insights provide contextual grounding and highlight practical challenges faced in operational environments.

5. Findings and Analysis

5.1 Technical Vulnerabilities

ADS-B systems remain susceptible to spoofing, jamming, and message injection (Costin and Francillon, 2012; Strohmeier et al., 2015) due to the lack of authentication and encryption. These vulnerabilities allow attackers to introduce false data or disrupt signal reception.

5.2 Operational Impact

The presence of unreliable or manipulated data can degrade situational awareness, leading to incorrect or delayed decision-making by air traffic controllers. This introduces safety risks, particularly in high-density or complex airspace environments.

5.3 Governance and System Gaps

Current approaches do not sufficiently integrate cybersecurity into operational procedures and decision-making frameworks. There is a lack of structured mechanisms for responding to degraded surveillance conditions and maintaining operational continuity.

6. Discussion

The findings highlight the limitations of purely technical approaches to ADS-B cybersecurity. While detection mechanisms are essential, they are insufficient in isolation. Operational environments require integrated approaches that combine detection, validation, response, and governance (Illiashenko et al., 2023; Dave et al., 2022).

The challenge lies in ensuring that ATM systems can continue to operate safely even when data integrity is compromised. This requires a shift toward resilience thinking, where systems are designed not only to prevent failures but to adapt and recover from them (Ojo-Oba, 2025; ICAO, 2019).

7. Proposed Resilience Framework

This paper proposes a resilience-oriented framework structured around five key domains:

- Threat Awareness and Monitoring
- Information Validation and Decision Support
- Operational Response and Control
- System Resilience and Continuity
- Governance and Implementation

The framework integrates technical, operational, and organisational elements to support robust and adaptive responses to cyber-physical threats in ADS-B systems.

8. Conclusion

ADS-B cybersecurity represents a critical challenge for modern Air Traffic Management systems. While vulnerabilities are well documented, there is a need to move beyond detection-focused approaches toward resilience-based strategies that support operational continuity and trusted decision-making.

This paper contributes by proposing a structured framework that integrates technical and operational considerations, providing a foundation for enhancing cybersecurity resilience in ADS-B-enabled environments.

Future research will focus on validating the framework through empirical studies and expanding its application within broader ATM and critical infrastructure contexts.

Ethics Declaration: This research involved preliminary practitioner insights collected through voluntary professional participation. The study does not disclose personal or organisationally identifiable information. Ethical considerations relating to confidentiality, professional sensitivity, and responsible research conduct were observed throughout the study.

AI Declaration: AI-assisted tools were used in a limited supporting capacity for language refinement, structural editing, and drafting support. All technical analysis, research interpretation, framework development, and final academic content validation were performed and reviewed by the author.

References

Ahmed, W., 2024. State-of-the-art security measures for ADS-B: Analyzing current protocols and future directions. *Premier Journal of Computer Science*, 1, 100005.

Costin, A. and Francillon, A., 2012. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Proceedings of Black Hat USA*.

Dave, D., Patel, R.S. and Shah, A., 2022. Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*.

EUROCONTROL, 2020. *Guidelines on cybersecurity for air navigation service providers*. Brussels: EUROCONTROL.

International Civil Aviation Organization (ICAO), 2019. *Aviation cybersecurity strategy*. Montreal: ICAO.

Illiashenko, O. et al., 2023. A survey on security and privacy of automatic dependent surveillance–broadcast (ADS-B) protocol: Challenges, potential solutions and future directions. *Sensors*.

Leonardi, M. et al., 2017. Detection of ADS-B spoofing based on multilateration and data fusion techniques. IEEE Transactions on Aerospace and Electronic Systems.

Nystad, K., Simensen, S. and Raspotnig, C., 2021. Investigating operative cybersecurity awareness in air traffic control. *Journal of Air Transport Management*.

Ojo-Oba, R.O., 2025. Cybersecurity challenges in aviation: Safeguarding airline operations against emerging threats. *Journal of Technology and Systems*, 7(5), pp.1–13.

Shi, Q., Caleb, T.D., Shao, S. and Kaabouch, N., 2026. Security of ADS-B and remote ID systems: Cyberattacks, detection techniques, and countermeasures. *Sensors*, 26(634).

Strohmeier, M., Lenders, V. and Martinovic, I., 2015. On the security of the Automatic Dependent Surveillance–Broadcast protocol. *IEEE Communications Surveys & Tutorials*, 17(2), pp.1066–1087.

Ukwandu, E. et al., 2022. Cyber-security challenges in the aviation industry: A review of current and future trends. *Journal of Aviation Security*.