International Civil Aviation Organization

A42-WP/479[1]
TE/189
29/7/25

WORKING PAPER

ASSEMBLY — 42ND SESSION

TECHNICAL COMMISSION

Agenda Item 24: Aviation Safety and Air Navigation Priority Initiatives

ADS-B AERONAUTICAL DATA SECURITY STRATEGY

(Presented by Colombia and supported by Latin American Civil Aviation Commission (LACAC) Member States[2])

EXECUTIVE SUMMARY

Automatic dependent surveillance — broadcast (ADS-B) technology has transformed air traffic management by delivering highly accurate, real-time data and more efficient airspace management. However, its reliance on unencrypted protocols makes it vulnerable to cyber attacks, as well as risks to data confidentiality. This can compromise the quality of information used by air traffic control (ATC) and expose the information transmitted to interference.

To mitigate these risks, comprehensive strategies should be developed that integrate multiple sources of surveillance data, both from collaborative and non-collaborative systems, correlating information to establish confidence levels and enhancing technological resilience and robustness. In addition, advanced cybersecurity practices and anomaly detection techniques based on big data and artificial intelligence (AI) should be implemented to assess and ensure information reliability. National laws and/or regulations should clearly define the boundaries between public and private use of such data, as well as the privacy implications for users of private and State aircraft.

This comprehensive approach will improve the quality and reliability of aeronautical data obtained using this technology, detect unusual patterns or discrepancies in altitude or position, including spoofing, thereby ensuring reliable information for ATC and safeguarding personal and confidential data in accordance with national legislation.

The latter aspect is particularly important, as it poses a new challenge for States, the aviation community, and some private companies, which will need to define the limits and consequences of the misuse of aeronautical data ADS-B under each State's data protection legal framework.

Action: The Assembly is invited to:

a) request ICAO to promote the development of national regulations establishing standards and mechanisms for the access, publication, and use of ADS-B information by private entities, safeguarding aviation privacy and safety without compromising the benefits of this technology;
b) request an analysis of the use of big data and AI for predictive automatic monitoring of ADS-B data quality, ensuring the accuracy of ADS-B data by correlating it with other systems within a

[1] Spanish version provided by Colombia.
[2] Belize, Bolivia (Plurinational State of), Chile, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay and Venezuela (Bolivarian Republic of).

multi-sensor program as part of regional air navigation plans, in order to mitigate the aforementioned risks; c) recognizing that data integrity is essential, and that any change to the transmitted information such as aircraft position and altitude could have serious consequences, data integrity controls and protocols (e.g., hashing algorithms, HMAC) should be introduced to ensure that the information has not been altered in transmission; d) in view of the risk to ADS-B data confidentiality in transmission over open radio frequencies, assess the feasibility of introducing ADS-B encryption, particularly in sensitive areas, so that only authorized systems can access the transmitted data; e) implement redundant surveillance systems (e.g., primary or secondary radar) that can provide back-up ADS-B data in the event of outages, and develop mechanisms to detect and mitigate jamming and other interference; and f) provide training for operators, technicians, and pilots on ADS-B-related risks and best practices to mitigate them, in order to raise awareness and improve responses to potential threats.	
Strategic Goals:	This working paper relates to the Strategic Goals *Every Flight is Safe and Secure*; *Aviation Delivers Seamless, Accessible, and Reliable Mobility for All*; and *No Country Left Behind.*
Financial implications:	
References:	Annex 17 — *Aviation Security* ICAO Document: *Aviation Cybersecurity Strategy* ICAO Document: *Cybersecurity Policy Guidance* ICAO Document: *Cybersecurity Action Plan* FAA website - PIA and LADD NBAA website Ali, B. S., Ochieng, W. Y., Schuster, W., Majumdar, A., & Chiew, T. K. (2015). A safety assessment framework for the Automatic Dependent Surveillance Broadcast (ADS-B) system. Safety Science, 78, 91–100. https://doi.org/10.1016/J.SSCI.2015.04.011 Jeon, D., Eun, Y., & Kim, H. (2015). Estimation fusion with radar and ADS-B for air traffic surveillance. International Journal of Control, Automation and Systems, 13(2), 336–345. https://doi.org/10.1007/s12555-014-0060-1 Jamming and Spoofing Protection for ADS-B Mode S Receiver Through Array Signal Processing. Lecture Notes in Electrical Engineering, 555, 184–204. https://doi.org/10.1007/978-981-13-7086-1_13 Smith, A., Cassell, R., Breen, T., Hulstrom, R., & Evers, C. (2006). Methods to provide system-wide ADS-B back-up, validation and security. AIAA/IEEE Digital Avionics Systems Conference - Proceedings. https://doi.org/10.1109/DASC.2006.313681

1. INTRODUCTION

1.1 The automatic dependent surveillance — broadcast (ADS-B) system has transformed air traffic management, providing greater accuracy, efficiency and availability of real-time data (updated every second), with lower installation and maintenance costs. It enhances airspace management, optimizing routes, improving congestion prediction, contributing to air traffic flow management (ATFM) and informing real-time operational decision-making. However, unencrypted transmission protocols make ADS-B vulnerable to various cyber and electronic risks that need to be addressed to ensure information integrity and avoid safety impacts.

1.2 Unencrypted transmission protocols expose ADS-B to cyber threats, the most significant being spoofing, phishing and jamming. This vulnerability compromises the integrity of the system and poses a significant risk to airspace and aircraft safety and security.

1.3 The confidentiality of ADS-B data is critical and requires special attention, particularly with regard to the protection of personal data, passenger identity, national security and confidentiality of operations. The dissemination, private exploitation or public disclosure of aeronautical data can affect the privacy of individuals, particularly in general aviation flights or private aircraft, and can compromise the safety of State flights, especially in international contexts. In this regard, it is essential to establish clear regulations governing the levels of access and authorization for the use, dissemination or commercialization of ADS-B information.

1.4 These factors highlight the importance of developing an ADS-B information security strategy that balances the need to use such data for purposes of safety, security and efficiency of operations with the duty to protect sensitive personal data in accordance with national legislation, as well as commercial exploitation of data, which requires an international standard of protection.

1.5 Effective mitigation of these risks requires comprehensive security strategies that encompass different aspects such as strengthening the technological infrastructure, developing tools for data analysis and establishing robust legal and regulatory frameworks. International cooperation and information sharing among States are crucial to address the challenges associated with ADS-B and to ensure the safety and efficiency of global airspace.

1.6 An effective and comprehensive risk mitigation strategy should combine data from collaborative (e.g., secondary radars) and non-collaborative (primary radars) surveillance systems. By correlating the information generated by these systems, it is possible to more accurately verify the targets transmitted by aircraft, both to ground stations and to low-Earth orbit satellite systems that send data to control centers. This approach enhances the resilience and technological robustness of the aeronautical surveillance system, improving its ability to withstand threats and ensure real-time safety.

2. DISCUSSION

2.1 ADS-B technology has transformed air traffic management by providing more accurate and abundant data, increasing airspace flexibility and supporting processes such as route management and billing. It optimizes airspace, improves safety, especially in areas with limited surveillance, integrates with big data and AI, and provides high-quality information for decision-making in ATM systems. In short, not only does ADS-B improve efficiency and safety, it also drives airspace modernization.

2.2 ADS-B technology relies on the transmission of data from aircraft and other applications such as global positioning systems. It transmits the data using open (unencrypted) protocols, making it vulnerable to: 1) cyberattacks targeting data and digital information; 2) electronic interference including electromagnetic interference on the radio frequency spectrum which can compromise the integrity of the data transmitted, with potential impacts on safety and security; and 3) unauthorized use of the aeronautical information.

2.3 The first element refers to cyber risks including spoofing, phishing, data tampering and denial of service. The second involves signal blockage, electromagnetic noise, global navigation satellite system (GNSS) spoofing and jamming.

2.4 The third element entails significant risk to personal privacy, the unauthorized use or disclosure of confidential data, particularly concerning general aviation, and the exposure of State aviation

to security threats. All these elements could pose risks to aircraft, ATC systems, airline reputation, and user privacy.

2.5 With regard to personal data privacy, the Federal Aviation Administration (FAA) has developed the limiting aircraft data displayed (LADD) programme and the Privacy ICAO Address (PIA) programme to address ADS-B privacy concerns. This programme enables owners of United States (U.S.)-registered aircraft to request an alternate, temporary ICAO aircraft address which will not be assigned to the owner in the civil aircraft registry.

2.6 The National Business Aviation Association (NBAA) has expressed concerns about ADS-B privacy, particularly for private and corporate aircraft operators, in line with this working paper. The Association notes that sensitive flight information can be exposed, enabling unauthorized tracking and data exploitation. The NBAA advocates for regulations that balance transparency with the protection of owners', passengers', and users' privacy.

2.7 Manufacturers have identified certain limitations in the PIA Programme that may discourage some operators from using it. For example, the program is limited exclusively to U.S. airspace and is therefore not valid for international flights, including across the Gulf of Mexico or the Caribbean. In addition, reverting from the ICAO address to the permanent one requires a technical maintenance procedure, which in some cases involves reprogramming the aircraft system. Consequently, the change cannot be made immediately. Another important limitation is that the aircraft could lose access to certain services provided by Aeronautical Radio, Incorporated (ARINC) and SITA that do not recognize the temporary address.

2.8 States have been strengthening their aeronautical surveillance systems through a comprehensive strategy that combines advanced technological infrastructure and the development of software driven by big data and AI. Strategies such as the implementation of a multi-sensor system with primary, secondary and ADS-B sensors in areas of high traffic density, together with security and cybersecurity measures for communication networks, offer technical solutions. At the software level, tools are being developed to characterize air traffic and detect anomalies automatically, improving the reliability of the information used by ATC. This approach optimizes aviation safety, security and efficiency, and should be part of regional air navigation plans.

2.9 With respect to the third matter of data privacy, States face regulatory and legislative challenges regarding the restrictions on the use of ADS-B–generated aeronautical information. Each State must define limits on the public visibility or third-party use of such data, considering the potential impact on the privacy, safety and security of aircraft, including general, private, and State aviation, and ensure legal protection in accordance with national data protection regulations.

2.10 The growing exploitation of aeronautical data, such as those provided by ADS-B through commercial platforms, raises serious questions about the privacy and safety impacts for aircraft users, both private and State. The lack of encryption and the broadcast features of ADS-B make flight information, including an aircraft's position and unique identifier, publicly accessible, compromising the safety of operations and passenger privacy. It is therefore essential for the aviation community, States, and private companies to cooperate in establishing regulations and mechanisms governing access to and use of this information, in order to protect aviation confidentiality and security without undermining the benefits of ADS-B technology.

2.11 For stronger regulation, it is important to have an updated international standard. States, operators, and private companies that publish aeronautical data should come together to develop measures,

through national legislation and civil aviation authorities, to ensure the protection of personal and sensitive data that may be at risk in the event of unauthorized disclosure, in accordance with national laws.

2.12 It is essential to address the impact on passengers of unauthorized disclosure and commercial use of aeronautical information on the internet. Only through constructive dialogue with data management companies combined with effective data use regulations, can the online exploitation of such information be mitigated. This approach helps safeguard the right to privacy and security for flights and passengers, particularly in private and State aviation.

2.13 In conclusion, while ADS-B is a vital tool for air traffic management, its vulnerabilities need to be addressed by States. A comprehensive strategy combining technological improvements, data analysis, and legal frameworks is essential to safeguard information and privacy. Regulations should also address the use of ADS-B data, particularly commercial disclosure of data pertaining to private and State aircraft, to protect the privacy of users and prevent security risks for States.

— END —