International Civil Aviation Organization

SEVENTH MEETING OF THE ASIA/PACIFIC AIR TRAFFIC MANAGEMENT AUTOMATION SYSTEM TASK FORCE (ATMAS TF/7)

Bangkok, Thailand 2-4 June 2026

Agenda Item 4: ATM Automation System Implementation Experience by States

4.3. Resilience consideration and contingency planning

ENHANCING CYBERSECURITY POSTURE FOR SINGAPORE AIR TRAFFIC MANAGEMENT AUTOMATION SYSTEM

Presented by Civil Aviation Authority of Singapore

SUMMARY

This paper presents an overview of Singapore's approach to strengthening the cybersecurity posture of its Air Traffic Management Automation System (ATMAS). It outlines the threats faced by mission-critical air traffic management systems in the evolving cybersecurity landscape, the key risks identified for Singapore's ATMAS, the layered technical and procedural control measures implemented, and the principal challenges encountered during the enhancement of a large-scale legacy system.

1. INTRODUCTION

1.1 Singapore operates an Air Traffic Management Automation System (ATMAS), known as the third-generation Long-Range Radar and Display System (LORADS III), to manage air traffic movements within the Singapore Flight Information Region (FIR). LORADS III integrates surveillance data, flight plans, and communication interfaces with multiple auxiliary systems, enabling real-time monitoring and effective management of air traffic operations.

1.2 In recent years, cybersecurity has assumed heightened importance due to the increasing frequency, sophistication, and impact of high-profile cybersecurity attacks targeting mission-critical and safety-critical systems. To support operational requirements and information exchanges, an ATMAS interfaces with external systems across both private and public networks which inevitably increases the system's attack surfaces.

1.3 Given the critical role of ensuring the safety, efficiency, and continuity of air traffic operations, such ATMAS represents a high-value target for adversaries, including well-resourced and highly capable threat actors. Cybersecurity incidents resulting in disruption, degradation, or unavailability of an ATMAS could have severe ramifications for airspace users and airports.

1.4 This paper presents an overview of the cybersecurity risks faced by Singapore's ATMAS, the control measures implemented to mitigate these risks, and the key challenges encountered in strengthening the cybersecurity posture of a large-scale, mission-critical legacy system.

2. DISCUSSION

Cybersecurity Risks

2.1 In view of the rapidly evolving cybersecurity threat landscape—encompassing new attack vectors, tactics, and techniques—Singapore conducts annual cybersecurity risk assessments on LORADS III. These assessments examine a wide range of plausible risk scenarios to identify vulnerabilities and inform the implementation of appropriate mitigation measures. The key cybersecurity risks identified include:

a. Targeted Attacks: Sophisticated cybersecurity operations, including Advanced Persistent Threats (APTs) conducted by nation-state actors or well-resourced groups, aimed at disrupting air navigation services or compromising critical air traffic management (ATM) functions.

b. Insider Threats: Malicious or inadvertent actions by personnel with legitimate system access, potentially leading to data compromise, unauthorised system changes, or operational disruptions.

c. Supply Chain Vulnerabilities: Risks arising from the introduction of malicious hardware, software, or code through third-party vendors, service providers, or maintenance activities.

d. Legacy System Vulnerabilities: Exposure resulting from outdated hardware and software components that may no longer be supported by vendors, limiting the availability of timely security patches and modern protective mechanisms.

e. Malware and Ransomware: The risk of malicious software infiltrating the system, potentially resulting in data compromise, degradation of system performance, service disruption, or denial of access through ransomware-based attacks.

f. Denial of Service (DoS) Attacks: Attempts to overwhelm system or network resources, potentially rendering ATM services unavailable and affecting the continuity of air traffic operations.

g. Remote Access Exploits: Unauthorised access through exploitation of remote connectivity mechanisms, particularly as remote operations and maintenance capabilities becoming more prevalent.

h. Data Manipulation: Unauthorised alteration of surveillance or flight data, which could lead to erroneous system outputs and adversely affect decision-making by air traffic controllers.

Cybersecurity Control Measures

2.2 To mitigate the identified cybersecurity risks, Singapore has implemented a layered set of technical and procedural control measures for LORADS III. These measures are designed to prevent, detect, and respond to cybersecurity threats across the system lifecycle. Key control measures include:

a. Privileged Identity Management (PIM) and Privileged Access Management (PAM): PIM/PAM solutions are deployed to strictly control, monitor, and audit the use of privileged accounts. These measures enforce strong authentication and least-privilege

principles, thereby reducing the risk of insider threats, unauthorised access, and credential compromise.

b. Endpoint Detection and Response (EDR) / Endpoint Protection Platforms (EPP): EDR and EPP solutions provide continuous monitoring of all endpoints, enabling timely detection of malware and advanced cybersecurity threats. These tools support rapid response and containment actions to minimise the impact of cybersecurity incidents.

c. Security Information and Event Management (SIEM): SIEM systems are used to centralise the collection and correlation of security logs and events across the ATMAS environment. This enhances visibility of anomalous behaviours, supports compliance monitoring, and facilitates the timely detection, analysis, and remediation of cybersecurity threats.

d. Multi-factor Authentication (MFA): MFA strengthens user authentication by requiring multiple verification factors prior to system access, significantly reducing the likelihood of unauthorised access resulting from compromised user credentials.

e. Firewalls and Network Segmentation: Network firewalls equipped with Intrusion Detection System (IDS) capabilities are deployed to regulate traffic flows between system zones and external networks. When combined with network segmentation, these controls limit lateral movement by potential attackers and isolate critical ATMAS components from less trusted environments. A Firewall Management System is also implemented to centrally manage firewalls and enables security teams to analyse network vulnerabilities, prioritize threats, and automate security policies creation and deployment.

f. Network Monitoring Systems (NMS): NMS provide continuous monitoring of network performance and availability, enabling early detection of abnormal traffic patterns and potential cybersecurity incidents, as well as supporting proactive maintenance and incident response activities.

2.3 In addition to the deployment of commercial off-the-shelf (COTS) cybersecurity solutions, Singapore conducts regular cybersecurity assessments and tests such as vulnerability assessments, penetration tests, host configuration reviews and compliance audits to ensure that LORADS III remains securely configured and resilient against emerging threats. Cybersecurity exercises are also conducted periodically to validate incident response procedures, as well as disaster recovery and business continuity plans.

Challenges in Upgrading Legacy Systems

2.4 Singapore encountered several challenges in implementing enhanced cybersecurity controls on LORADS III, a legacy system originally designed for a service life of at least 15 years without major technology refresh. Given the system's scale, complexity, and the extent of upgrades required, the implementation was expected to entail prolonged system downtime. However, stringent operational requirements to maintain 24/7 air traffic services significantly constrained the availability of extended downtime for system upgrades.

2.5 To address this, Singapore adopted a phased upgrade strategy instead of a single "big-bang" implementation. The first phase focused on upgrading the operating system (OS) and ATMAS application, while the second phase involved the migration and onboarding of LORADS III into a new subsystem comprising modern system monitoring and commercial off-the-shelf (COTS) cybersecurity solutions.

2.6 LORADS III is purpose-built to support mission-critical ATM operations and use proprietary OS and software to achieve optimum system performance. As with many legacy systems, LORADS III is subject to technical constraints arising from outdated hardware and software that do not natively support modern cybersecurity solutions. The use of proprietary products in the system also hinders integration with latest COTS products out of box. This necessitated custom integration efforts and, in some cases, the adoption of compensating controls. Furthermore, many COTS cybersecurity products are designed to operate only on the latest OSes. To address these challenges, Singapore worked closely with the system's original equipment manufacturer (OEM) to assess compatibility and select suitable cybersecurity solutions aligned with the OEM-customised OS and middleware.

2.7 During the first upgrade phase, LORADS III systems were migrated to a newer OS. This required upgrading the underlying hardware and porting the ATMAS application to a version compatible with the selected OS. To facilitate the upgrade while minimising operational impact, a dual-boot configuration was implemented for each system, allowing operation under either the existing or new OS environment via a system reboot. This approach enabled the upgrade work to be broken down into smaller, manageable increments carried out over multiple short downtime periods without disrupting air traffic control operations.

2.8 For the second upgrade phase, the new system monitoring and cybersecurity COTS solutions were first deployed as a standalone subsystem with out-of-band network infrastructure. Following completion of the initial upgrade phase, LORADS III is progressively integrated into this subsystem with each cybersecurity capability being onboarded incrementally. Given the real-time and mission-critical nature of LORADS III, sufficient monitoring periods are required at each stage to ensure system performance and operational integrity are maintained without degradation.

2.9 In addition, resource constraints—including limited specialised cybersecurity expertise and budgetary considerations—pose challenges to the timely and comprehensive adoption of advanced cybersecurity controls.

3. CONCLUSION

3.1 Singapore's experience demonstrates that strengthening the cybersecurity posture of mission-critical ATMAS requires a risk-based and defence-in-depth approach, underpinned by regular assessments, layered technical and procedural controls, and close coordination with system manufacturers and stakeholders. Such measures are essential to safeguard the confidentiality, integrity, and availability of ATMAS functions and to support the continued safety and continuity of air traffic operations.

3.2 At the same time, the paper highlights that enhancing cybersecurity in large-scale legacy ATMAS environments is complex and resource-intensive, particularly where operational continuity must be maintained. A phased implementation strategy, supported by compensating controls and continuous monitoring, can enable meaningful security improvements while minimising disruption to critical air traffic services.

4 ACTION BY THE MEETING

4.1 The meeting is invited to:

a) note the information contained in this paper; and

b) discuss any relevant matter as appropriate.

– – – – – – – – – – –