International Civil Aviation Organization

Third Meeting of the Asia/Pacific Air Traffic Management Automation System Task Force (APAC ATMAS TF/3)

Video Tele-Conference, 8– 10 June 2022

Agenda Item 4: ATM Automation System Implementation by States
4.3 Development of New Technology

ATMAS CYBERSECURITY DESIGN IN BRIEF

(Presented by China)

SUMMARY

This paper presents the current cybersecurity status of Air Traffic Management Automation System (ATMAS) in China, and the brief design on 3 key aspects of cybersecurity in common between ICAO Doc 9985 and Chinese cyber security standard serial (GB/T 22239-2019).

1. INTRODUCTION

1.1. The ICAO Doc 9985, Air Traffic Management Security Manual, is the guideline for the design of Air Traffic Management Automation System (ATMAS) security. It proposes the network information security control strategy of ATMAS from 9 aspects.

1.2. The Chinese serial standards of Multiple Level Protection of Information Network Security (GB/T 22239-2019) v.2.0, was promulgated in 2019, in which the 3rd level protection is requirements set to ATM automation system from 10 aspects.

1.3. These 2 standards resemble in below 3 key technical aspects by minimum. This document reflects the Chinese design on these aspects, particularly the first 2, in according with GB/T 22239-2019:

ICAO document 9985		Multiple Level Protection of Information Network Security （GB/T 22239-2019）v.2.0
ATM system infrastructure protection	=>	Security of communication network, boundary security, secure computing network, security management center
Monitoring and Audit	=>	Security management center
ATM security operation	=>	Security maintenance and operation

2. SECURITY STATUS AND RISK PATH IN ATMAS

2.1. The ATM automation system is a critical infrastructure of air traffic operation, it bears characteristics of high continuity, prompt response, no single point failure permit, and sensitivity to transmission latency. With more and more amount of data connected to ATMAS, and increasing complexity network topology by interaction with other systems, the network security of ATMAS becomes a key problem to resolve against various potential attacks.

2.2. In past a few years, the ATC operating lines of ATMB have successively carried out audit of ATM automaton systems cyber protection. The results show that the ATM automation system has a rather high degree of protection in terms of physical environment control, and also established corresponding level of administrative regulations for information management. On the other hand, some legacy systems were designed several decades ago, those are lack of design against unauthorized connections, intrusion detection and protection, etc. There are high-risks in aspects of the secure computing environment, boundaries security, and security management centers, such as lack of effective risk dispersion mechanism in the subnetwork design, no supervision over the operation of overall ATM automation system, or traffic, logs, security events, user behavior, and so on, not to mention the correlation analysis among them.

2.3. Due to its operational characteristics, ATM automation system usually runs in a closed environment as an individual network without intervention of Web. The cybersecurity risks typically come from three paths:

- **Data access and interaction risk:** The system connects multiple data sources (ADS-B data, meteorological data, Flight plan, etc.) through network boundary or interacts with multiple other aviation sub-systems that are out of control of ATC lines.
- **Risks introduced by operation and maintenance (O&M) terminals:** O&M personnel can access and control any server or workstation by remote login, and they use portable media to upload/download files. There is a risk of human mal-operation.
- **Risk introduced by workstation**: air traffic controller team is larger than that of system operator, and use of business system interfaces (HMIs) on workstation bears the potential risk of connecting remotely to the core system or entering the physical operation room.

3. THE FRAMEWORK OF ATMAS NETWORK SECURITY DESIGN

System network security design overview

3.1. To downgrade the risks of ATM automation system, the network must be divided into zones, in which functions are protected in depth, thus the concept of security domain is introduced (see Figure 1).

3.2. The whole ATM automation system is divided into the following 6 logical security domains according to their functions: external signal zone, data segregation zone, core operation zone, security management zone, system maintenance zone, and remote subnet zone.

3.3. Segregation measures and security policies between the 6 logical security zones:

- **External signal zone:** various types of external signals required for ATM automation system operation, such as flight plans, etc., as well as output of operational data from ATM automation system to other external subsystems. The input signals come from other aviation subsystems, transmitted over dedicated fiber cables. As untrusted sources, they must be physically and logically segregated from the boundaries of ATMAS core network.

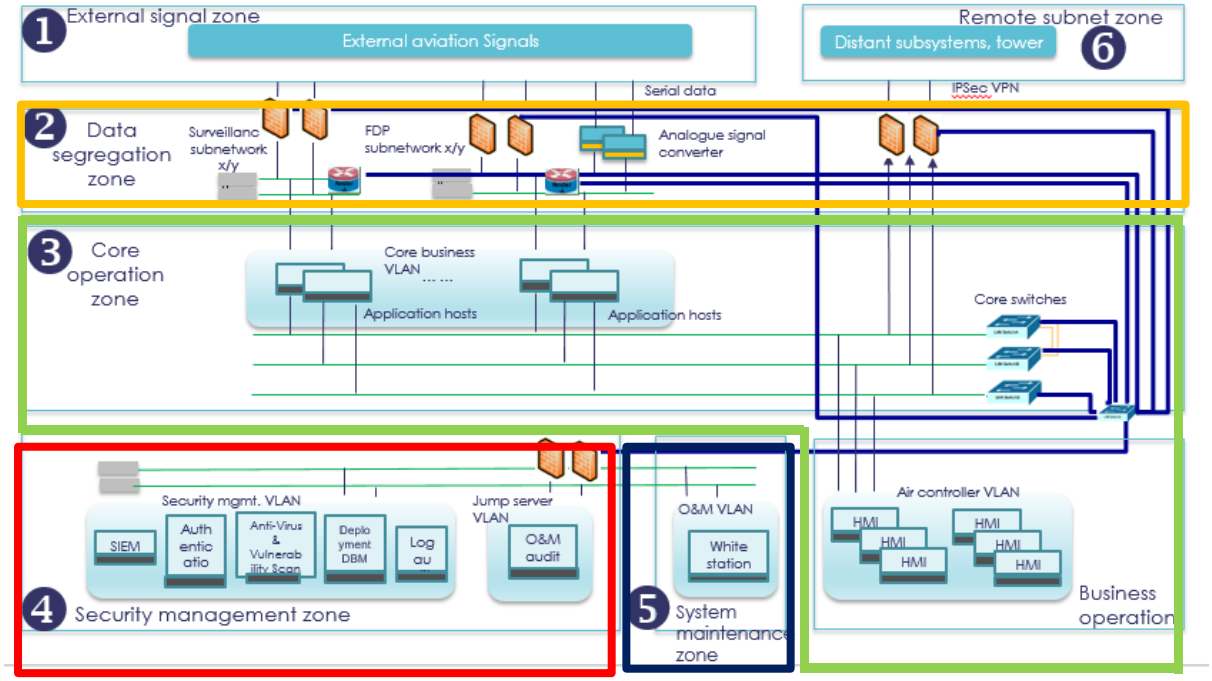

Figure 1: Security domains segregation for ATMAS network.

➢ **Data segregation zone**: it provides boundary protection, segregates various input and output signals from the core operation network, boundary intrusion detection, filter prevention, and reports various security events to the security management center. Segregation is an effective mean to avoid deploying critical components next to network boundary.

The dedicated equipment for boundary protection can be firewall for IP traffic, proxy servers, or gateways, forming comprehensive processing capability against external signals or distant communication.

➢ **Core operation zone**: deployment of all backend data processing servers of ATM automation system, the front-end HMI workstations, switching network, system monitoring servers, maintenance servers and other auxiliary O&M seats. All real-time and historically trusted operating data are stored in this zone too.

➢ **Security management zone**: responsible for managing the security status of the entire network. A new D sub-network is established for security management, via which all security events or running logs are transmitted to the corresponding servers located in the security management zone for further analysis. Meanwhile, assets of ATM automation system are recorded, tracking and here, as well as data associated with critical infrastructure and security management.

➢ **System maintenance zone**: The O&M zone is in separate network segments from the security management zone and core operation network zone. ACL, VLAN, and MAC address and Firewall rules are deployed to achieve filtering and connections segregation. The system maintenance process as well as user log in events are recorded and audited by jump server; anti-virus measures are deployed on each maintenance seat (aka white station). Overall all security statuses are presented on the display.

➢ **Remote subnet zone:** Distant communication between subnets (such as terminal center to tower systems) within an ATC for flight plan synchronization or configuration data synchronization. In principle such cross-regional communication should be protected in case

transferred over non-dedicated links.

Hardening of the core operation zone

3.4. User Account and rights control

- Role-based access control (RBAC) is applied, and users are divided into 2 groups: business users (i.e., air traffic controllers) and system administrators. Restricts business user accounts to access only business operation and only via HMI interface, i.e. cannot access core network system neither can use the system administrator account.

- System administrator rights are dispersed to 3 roles: system administrator, managing all user accounts and network issues, but no rights to manage network security. The security administrator is dedicated to security deployment of the network, and inspection of security status, discovers vulnerabilities in design, deployment, or O&M. The audit administrator's role is to audit independently all network security logs, security incidents, alarms, and can assess in neutral. Administrator ID must be two-factor authenticated.

3.5. Operating system upgrades and hardening

The transfer of critical files within ATM automation system must be securely authenticated beforehand and protected during transmission (e.g. SSH), including but not limited to online configuration files, management files, log files, etc.

3.6. Vulnerability Scan

Construct a complete vulnerability database and update mechanism, conduct routine inspections against all equipment in an ATM automation system, and analyze and test the newly released patches. Based on the testing results, follow corresponding steps in the predefined security response process, execute follow-up observation, immediate repair, shut down certain connections and so on.

3.7. Malicious code detection

The endpoints of the ATM automation system must have adequate antivirus protection against malicious code and be able to detect and respond promptly. This can be achieved by deploying secure gateways around the boundaries of the core network zone or Endpoint Detection and Response (EDR) on the endpoint.

3.8. Backup management:

Different types of data are backed up by a variety of means.

- Critical data in O&M equipment, data in the security management platform, jump server, and traffic monitor, are regularly backed up to local storage.
- The configuration parameters of operation systems, network devices, file systems and important data files are regularly backed up to local storage.
- Save a local backup of the software installation package while in installation.

3.9. Portable media management

Administrative regulation must be defined to manage portable media to avoid risks introduced to the system by uploading and downloading:

- Each portable media must be allocated with an individual ID; it is dispatched by the security operations team only and returned after usage.
- The USB stick belonging to ATC team cannot be taken out of the office area, and neither can that belongs to other offices be carried into the ATC office.

➢ The daily O&M portable media can only be used in the O&M zone, unless specially approved by the security administrator for another purpose.

➢ • Portable media must be disinfected on the O&M white station before use.

➢ Portable media must be completely erased or securely overwritten before they are scrapped or reused to ensure that sensitive data and licensed software on the device cannot be recovered and reused.

3.10. Traffic monitor

Traffic packets are collected in backbone of the core network, and abnormal patterns are detected promptly, such as abnormal payload, abnormal flow direction, abnormal requests, and so on. The directly collected data is sent to the security management center for analysis.

3.11. Source code audit

The ATC manufacturer should provide a system critical code audit certificate issued by a trusted third-party auditor. If it cannot be issued, the O&M department signs a relevant agreement with the ATMAS manufacturer to cover its potential risk.

Security management center

3.12. There may deploy hundreds of various types of equipment, many nodes in a large ATM automation system with complex network topology and physical connections, which lead to a variety of potential risks. These risks can be effectively managed by collecting logs and security events of devices, and analyzing the correlation between multiple dimension alarms. In a typical security management center, there are by minimum log audit server, O&M audit server, database audit server, and security management server, jointly they buildup management capability for the entire network. Figure 2 is a topology diagram of a security management center managing multiple sets of ATM automation systems.

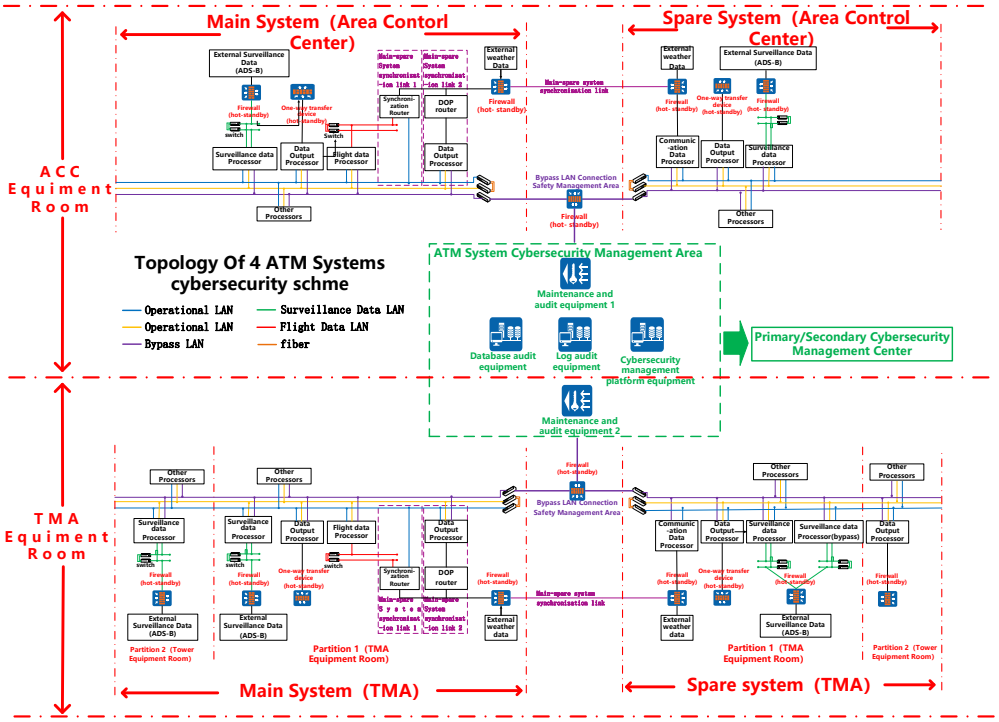

Figure 2: Centralized security management zone.

3.13. Functions of each component in the security manager zone:

- **Log audit server**: centralized processing point for logs pushed by various types of equipment into (or pulled by) ATM automation system.

- **O&M audit server**: with the deployment of the O&M audit server, the path of maintenance is as following hops: maintenance personal on maintenance white station -> jump server -> O&M audit server -> ATC node. SSH protection is deployed between each link along the path.

- **Database audit server**: when there is generic databases such as Oracle, database audit configuration should be placed. Log file of ATM automation system database should be pushed via dedicated security D network to database audit center. The firewall should be configured with corresponding rules to allow audit server to receive such logs.

- **Security management server**: identifying, analyzing and alarming various security events occurring in the network, monitoring the traffic inside the ATM automation system, analyzing the correlation of various information, and alarming suspicious action, and submit to the upper level security management center.

- Visual presentation security status of the whole network in one display.

3.14. It is worth noting that types of equipment, data structures, information patterns, and network topology of different ATM automation systems are unlikely the same, Therefore, the software in servers of the security management center must be double developed to perform customized correlation analysis for main and spare system separately.

3.15. ATM automation systems is a kind of stable and rigorous operating systems (OTs) running on top of IT networks with definitive output at any single time point. This makes its security management rules different from typical IT systems. These include the following:

- **Analyzer library:** It needs mature analysis software and complete sets of analyzers for the operation mechanism of ATM automation system. Only by years of practice in the aviation industry, these analyzers can conduct high reliable and trusted output that builds a foundation of system safety.

- **Customized software component library for docking with various types of safety equipment:** Complete and ready libraries of adaptation software with all kinds of well-known security equipment for smooth deployment.

- **Correlation analysis rule base:** Pattern recognition according to the operation baseline of the ATM automation system, properly customized based on correlation of analysis rules, to generate efficient and meaningful alarms. For complex attack such as Advanced Persistent Threat (APT), correlation needs to be defined based on long term learning on anomalous behavior captured by several security subsystems jointly.

- **Cyber Threat Integrator:** Risk modeling and known threat methods against ATM automation systems as a foundation, and construct protection is built based on that.

- **Secure Orchestration and Automated Response SOAR:** Security experts jointly work with ATC business experts to orchestrate and collaborate on the operating patterns of ATM automation system, and design automated response processes and workflows to improve the efficiency, effectiveness, and consistency of security O&M. This automated process, often based on machine learning capabilities, can quickly process incoming security incidents, including triage,

containment, remediation, etc. SOAR is not only workflows, but the combination of tools in coordination with proper information flow, as well as the organization of people flow. It must be very carefully defined by ATC security senior.

4. CONCLUSION

4.1. Given its complexity, the construction of security protection for ATM automation system must be developed in phases gradually and continuously, and cannot be achieved overnight.

4.2. The design discussed here covers only the technical aspects as the initial stage of construction; to deploy security of ATM automation system, it should also establish relevant administration regulations.

4.3. The construction of network security's O&M capability is the necessary means for security protection to achieve long-term safety and stability of ATM automation system. It is necessary to track and analyze system security risks, and to monitor system's protection from laws, regulations, personnel control, and technology updates, to improve continuously system security level.

5. ACTION BY THE MEETING

5.1. The meeting is invited to:

a) note the information contained in this paper; and

b) discuss any relevant matter as appropriate

– – – – – – – – – – – – –