International Civil Aviation Organization

Fourth Meeting of the Asia/Pacific Air Traffic Management Automation System Task Force (APAC ATMAS TF/4)

Bangkok, Thailand, 28 – 30 June 2023

Agenda Item 4: ATM Automation System Implementation Experience by States

4.4 Development of New Technology

RESEARCH ON STANDARDIZED CYBERSECURITY PROTECTION SOLUTION FOR ATM AUTOMATION SYSTEM

(Presented by China)

SUMMARY

This paper presents achievements of CAAC in the implementation and standardization research of cybersecurity for ATM automation systems.

1. INTRODUCTION

1.1 In 2013, ICAO published Doc9985, *ATM Security Manual*, which provided nine control categories for ICT cybersecurity. It notified that NCASP should focus on building a comprehensive cybersecurity strategy in three aspects:

a) The protection of systems against unauthorized access.
b) The prevention of tampering with systems.
c) Detection of attacks on systems.

In technical controls and the application of security equipment, high-availability solutions should be selected.

1.2 Based on Doc 9985 and national regulations, CAAC published *Baseline for classified protection of cybersecurity in civil aviation (MH/T 0076–2020)*, in 2020.

1.3 According to the guidelines of ICAO Doc 9985 and CAAC standards, ATMB of CAAC has been continuously committed to research on cybersecurity of the ATMAS and implemented cybersecurity upgrade in some ATMAS. Following a comprehensive review of experiences, the standardized cybersecurity protection solution has been given out.

2. DISCUSSION

2.1 Since 2020, ATMB of CAAC has been working with equipment suppliers to carry out cybersecurity upgrades and evaluations of the ATMAS in multiple locations, as shown in Table.1. In

addition, cybersecurity facilities have been incorporated as an essential component in the system design, integration, and acceptance of the ATMAS.

Tal.1 Cybersecurity implementation in recent years

Year	System location	Vendor/Model	Describe
2020	Sanya	LES NUMEN	Upgrade
2021	Zhuhai	BEST SkyNET-X	Upgrade
	Zhanjiang	CDATC AirNet	Reconstructed
2022	Zhuhai	LES NUMEN	Upgrade
	Ningbo	CDATC AirNet	Reconstructed
2023	Beijing	LES NUMEN	Upgrade
	Anhui/Yantai/Changsha/Ningbo		Upgrade
2023	Guilin	BEST SkyNET-X	Upgrade
	Nanchang、Sanya	CDATC AirNet	Reconstructed

2.2 The cybersecurity architecture for the ATMAS has been established as shown in Figure.1. The security technology system is the foundation for achieving cybersecurity, and the core of the technology system is the construction of "One center, Triple protections", includes:

a) Communication network security.
b) System boundary security.
c) Computing environment security.
d) Security management center.

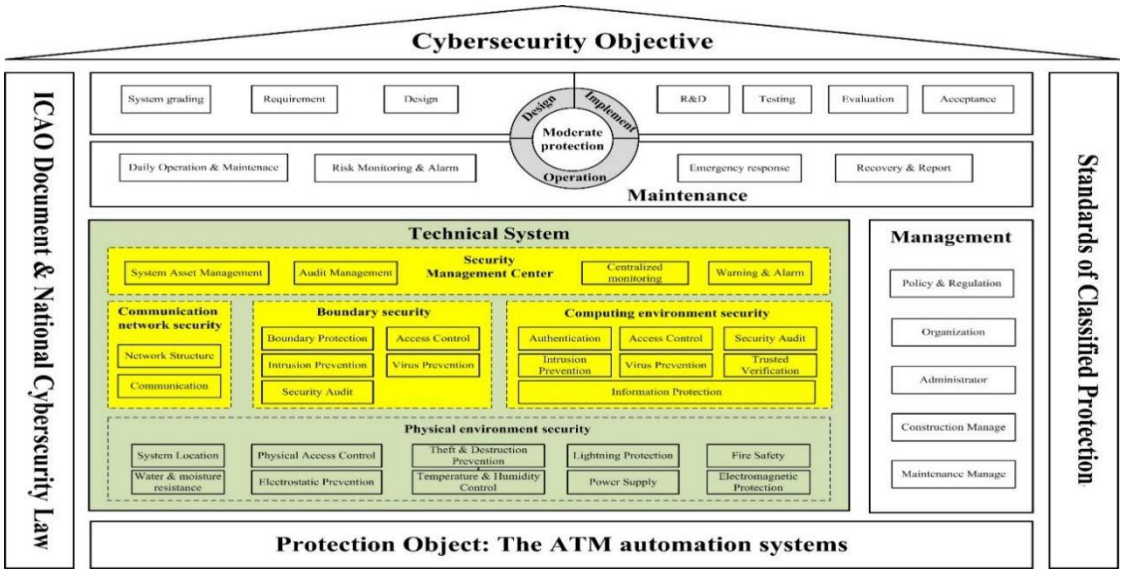

Fig.1 Cybersecurity architecture for ATMAS

2.3 In 2022, ATMB of CAAC compiled "*The technical guidelines for classified protection of cybersecurity in ATMAS construction*" to give a standardized cybersecurity protection solution for reference.

2.3.1 Design Principle

The solution is based on the concept of "One center, Triple protections" with design principles as follows:

a) High stability, reliability, and low delay while meeting the essential cybersecurity requirements, security devices or products should minimize the resource usage to

reduce the impact on the ATMAS.

b) Balancing linkage and independence. When dividing security management zones and subnets, the interconnection between the two should be taken into consideration, ensuring timely detection and handling of security incidents through security monitoring and auditing.

c) The cybersecurity solution should be designed as a part of the ATMAS to be implemented together with the system and convenient for maintenance. The network environment of the system should be considered to keep a balance between security and economy and avoid excessive defense.

d) Compatible with various models of ATMAS provided by different vendors, as well as its scalability to accommodate upgrades and developments of ATMAS.

2.3.2 Security Zone Division

The division of security zones is the basis for the solution. Based on the network structure of the ATMAS, security zones should be divided to determine the hardware of security devices, deploy protection policies, and define the network behaviors and control measures of each zone.

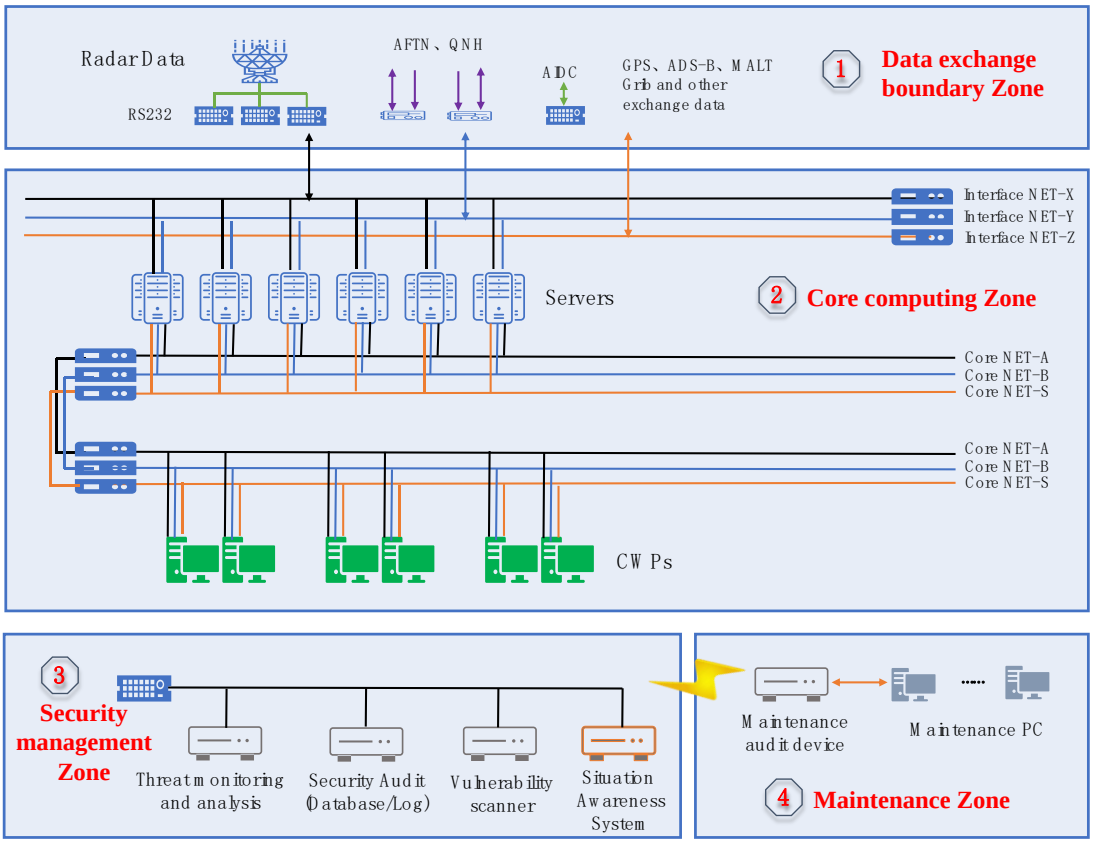

Fig.2 Cybersecurity zone division

As shown in Figure.2. It is recommended to divide the ATMAS into four or five security zones:

a) The data exchange boundary zone provides data inputs (radar data, AFTN messages, meteorological data, etc.) for the ATMAS, while outputting operational data to external systems (the backup ATMAS, the Tower ATMAS) for data exchange. This zone is a high-risk area for cybersecurity, in which the security devices and policies should be laid out with emphasis.

b) The core computing zone includes servers, position workstations, technical

maintenance terminals, and the A/B/S core networks. This zone is a key protection object for cybersecurity.

c) The maintenance zone is built to reduce security risks brought by maintenance behaviors such as remote access, files copying, etc. Use the security devices in the zone to manage the maintenance accounts, authorize system administrators, and connect to external storage devices.

d) The security management zone uniformly monitors and manages the network security of the air traffic control automation system. Through an independent data flow collection network, various security events of the air traffic control automation system equipment are transmitted in real-time to the area for intelligent correlation analysis, identifying network security issues in the ATMAS, and providing alarms or responses.

e) The system interconnection zone is designed for the ATMAS with a remote structure composed of multiple subsystems (TCU). This zone works as a buffer between the main system and subsystems, with a clear boundary for deployment of relevant isolation measures.

2.3.3 Security Devices

The hardware configuration of security devices is shown in Table.2.

Tal.2Cybersecurity devices configuration

Zone	Devices	Function
Data exchange boundary zone	Firewall	isolation, border protection, access control, antivirus prevention, intrusion prevention
Security management zone	Threat monitoring and analysis device	Work as sensors for flow collection and pre-analysis
	Log audit device	Security audit
	Database audit device	
	Vulnerability scanner	Check for security vulnerabilities in the system
	Network Situation Awareness System	Real time monitoring and warning
Maintenance zone	Maintenance audit device	Maintenance audit, maintenance account management
	Maintenance computer	Files Copying and importing

2.3.4 Security Policy Configuration

While the implementation of security devices, the security policy should be deployed as follows:

a) In the multi-zone system, IP address segmentation management should be implemented for different subsystems of the system. If necessary, Layer 2 isolation can be implemented through technologies such as VLAN

b) Access control policies (ACL) must be strictly deployed for data entering and exiting the system boundary and the system partitions. Based on service communication requirements, check the source address, a destination address, source port, destination port, and communication protocol required by the protocol policy

c) All assets, network addresses, and users of the system should be authorized in advance. Unauthorized users should be prohibited from performing any operation such as communication and access in the system through the access control policy.

d) Considering the construction cost, the primary and backup ATMASs can share the equipment in the security management zone, but it should be confirmed that there is no IP duplication or conflict; The communication network between the security management zone and the primary and backup ATMASs should be physically or logically separated to ensure the independence of the core network for primary and backup automation business.

2.4 Next Step

2.4.1 CAAC ATMB will carry out cybersecurity constructions and upgrades of the ATMAS according to the standardized solution.

2.4.2 CAAC ATMB will track the implementations of the ATMAS cybersecurity in China, and continuously improve the technology system, gradually establishing the maintenance and management system.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) encourage countries and regions to evaluate the applicability and extensibility of the solution proposed by this paper.

– – – – – – – – – – – –