

(Presented by China)



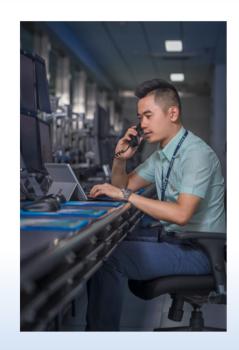


Biography of Mr. Gong Xinyu

Mr. Gong Xinyu, Senior engineer Chongqing Air Traffic Management Sub-bureau, CAAC

Mr. Gong Xinyu is working in CNS department of Chongqing ATM Sub-bureau. He has a great deal of experience in the system implementation, technical support and maintenance. Since 2018, he has been dedicated to the cyber security research of ATMAS. He is also one of the security management experts of ATMB.

Mr. Gong Xinyu has given SP/IP on the cyber security item in the ICAO ATMAS SYMPOSIUM (2018), ATMAS TF/1 (2020), ATMAS TF/4 (2023).







INTRODUCTION

Part1: Background

Part2: Research of the cybersecurity

Part3: Integrated cybersecurity solution

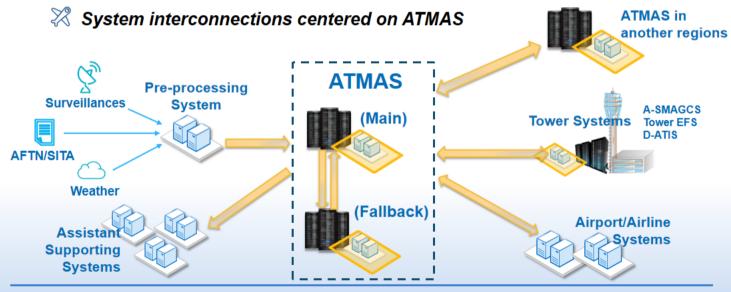
Part4: Implementation & Next step







1 BACKGROUND

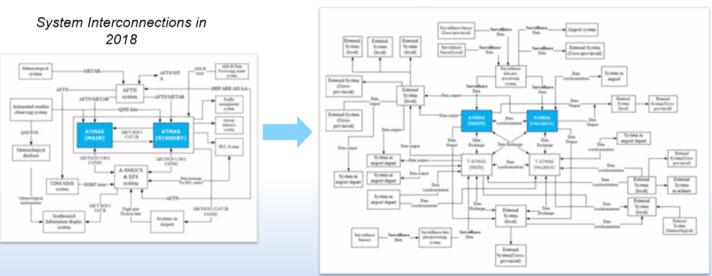






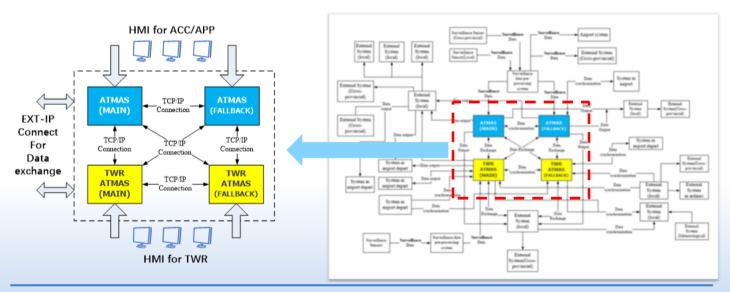
More external systems are connected to the ATMAS, ANSP have to face the increasing challenges in cyber security

System Interconnections in 2024





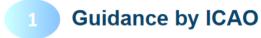
The Tower ATMAS will work together with ATMAS to play a central role for dataexchange. Cyber-security of the Tower ATMAS should be considered











Cybersecurity Policy **ATMAS IGD Network Infrastructure User Account Management** System Development Life Cycle Removable Media Control Software Security Patch Management **Physical Security Measures** Response to Cyber Security Incidents



Air Traffic Management Automation System

Implementation and Guidance Documen

4.8 Cyber Threats and Mitigation

4.8.1 General Description

With the extensive deployment and closer interconnection of Commercial OST-The-Schell (COTS) information and Communication Tracknology (CTS) systems which is bail on common standards rather than on the conventional proprietary equipment, the Newigation Service Provident (ASSNP) have been facing increasing challenges in protecting their critical influstructure and manage potential risks arising from cyber security fluents.

To address the growing concerns on cyber security threats, ICAO Jia extended in SAEPs with Assets I on Security, with the upplement as in ICAO Dec. 8973. "Assisten Security Massist" which is not not the avaisation Security Massist" which asts not the avaisation Security Massist" which is addition, ICAO Joachida Que 19875. "ATM concluding tyber necessity in ATMA ISA. In addition, ICAO Joachida Que 19875." ATM infrastructure from cyber attacks. States/Administrations are encouraged to present the infrastructure from cyber attacks. States/Administrations are encouraged to present the appropriate level of compliance to the cyber security control engineeries an astated in the ICAO documents and make collaborative efforts to effectively address cyber security threats. ICAO and other international organizations have been presenting the upsetting of a CAO and other international organizations have been presenting the upsetting of the security in ATC systems with their various and of Excellence in Cyber security.

4.8.2 Cyber Security Management

States/Administrations are encouraged to devolen cyber security management, which adopts a proactive and optention if agreement for protecting the increasing digitation of ATS against cyber threats, through the establishment of Cyber Security Manual, Cyber Security Manual, Cyber Security Manual, Mandbook and User Account Management Policy. The above-mentioned decuments should be developed in accordance with relevant provisions in ECAO Annex 15 and Dec 1998 to provide protection of the author-printed ATMAS against cyber threats and interference. Key elements of enhanced controls on cyber security are as follows for reference:

a. Cyber Security Policy

States/Administrations should establish their own Cyber Security Policy to mitigate cyber threat. Dedicated committee or working group on cyber security with regular meetings is encouraged to set up for reviewing policies and steering the implementation of cyber security control measures throughout the whole life cycle of ATMAS.

b. Network Infrastructure Protection

Introperation among ATMAS and other ATS systems for information exchange in newinfulor. Frosterior protection of the backbone data network of ATMAS in essential to ensure its operation. Multi-tier defence-in-depth scheme for external TCPFB unional content of the other comprising comprising network optiment, firewalls. Network Intrasion Detection (NIDS) or Network Procession System (NIPS) is registered to strengthen the





The ANSP should be content with cyber security measures according to the NCASP and national programs





Baseline for classified protection



Critical information infrastructure protection

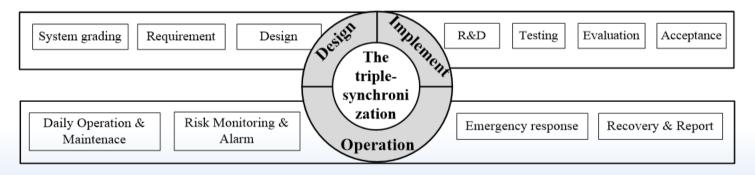


Since 2020, ATMB of CAAC has been working with equipment suppliers to carry out cybersecurity upgrades and evaluations of the ATMAS in multiple locations

| 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 | LES INDIVIEN | Upgrade |
| 2023 | Guilin | BEST SkyNET-X | Upgrade |
| | Nanchang、Sanya | CDATC AirNet | Reconstructed |



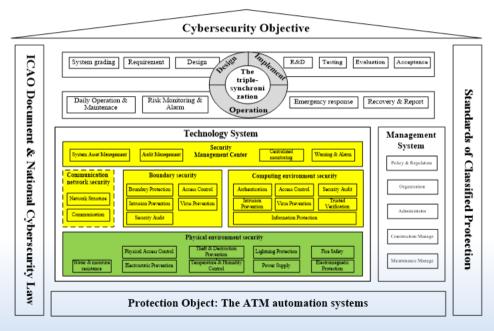
- Since 2020, ATMB of CAAC has been working with equipment suppliers to carry out cybersecurity upgrades and evaluations of the ATMAS in multiple locations
- Cybersecurity facilities is required to be incorporated as an essential component in the system design, integration, acceptance, and O&M of the ATMAS





- The cybersecurity architecture for the ATMAS has been established
- Technology system is the foundation

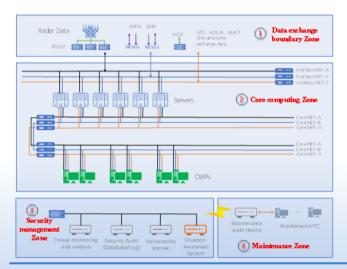
One Center
Triple Protections

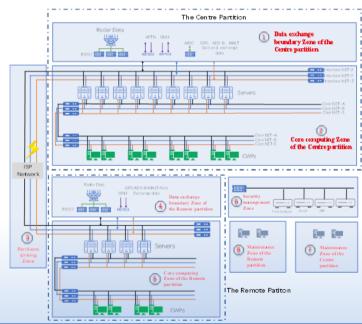




Technical Guidance for Classified Protection of Cybersecurity in ATMAS construction

- Security Zone Division
- Devices configuration

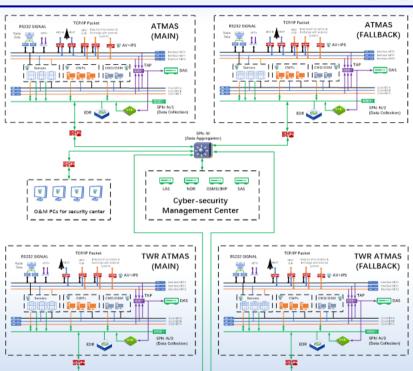








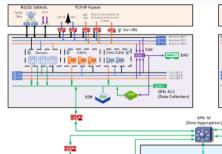
- Design based on the Technical Guidance, in 2023
- Integrated solution for ATMAS and Tower ATMAS considering the similarity of system topologies
- Applicable to ATMAS with only one partition
- Being implemented in the Chongqing ATC center, in 2024





Data exchange boundary Zone (MAIN ATMAS)

Zone (MAIN ATMAS)



9 9 9 9

O&M PCs for security center

RE22 SIGNAL
TCP/IP Packet

TCP/IP Pa

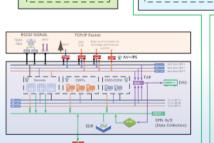
Data exchange boundary
Zone
(FALLBACK ATMAS)

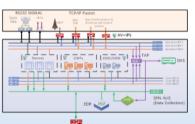
Core computing Zone (FALLBACK ATMAS)

Maintenance Zone (Shared)

Data exchange boundary Zone (MAIN TWR ATMAS)

Core computing
Zone
(MAIN TWR ATMAS)





Security Management Zone

(Shared)

Data exchange boundary
Zone

(FALLBACK TWR ATMAS)

Core computing Zone (FALLBACK TWR ATMAS)

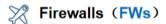
OSMS/IMP

Cyber-security Management Center



1

Protection in the system boundary

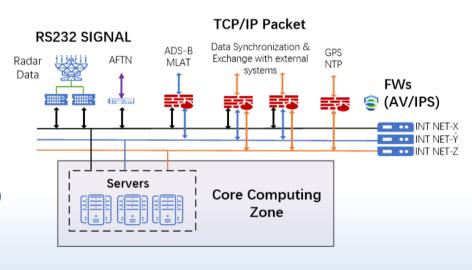


Deploy ACL to authorize access for the trusted connections

Black lists to intercept and block cyber threats

Intrusion Prevention System(IPS) & Anti Virus(AV) module

Isolation between security zones





Protections in the core computing zone

Database Audit System (DAS)

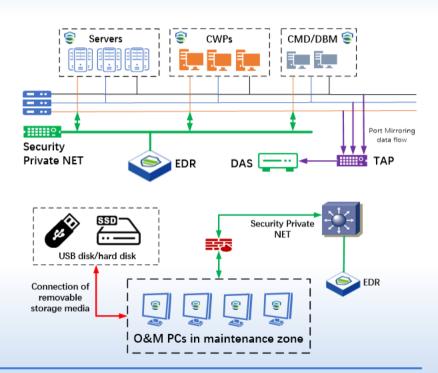
Alerts on unauthorized database access and data tampering

EDR Protection

Virus detection in the servers and workstations

Detect unauthorized terminal accessing

Risk Control on the connection of removable media





3

Devices in the security management zone (center)

X LOG Audit System (LAS)

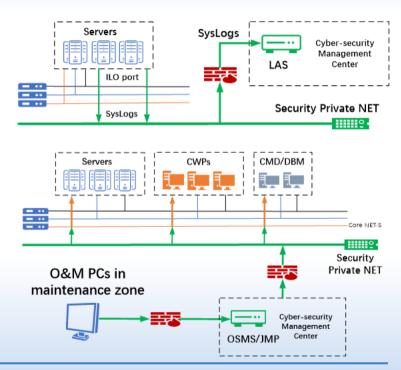
Collect system logs from servers Alerts for abnormal log messages

O&M Security management System (OSMS)

Jumper for O&M staff to remotely access to the servers and workstations (CWPs)

Recording O&M behaviors

Management of O&M administrator accounts





3

Devices in the security management zone (center)

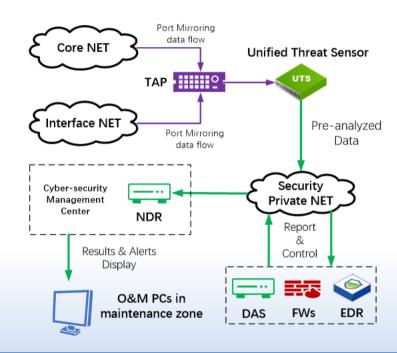
Traffic Monitoring and Analysis System (NDR+UTS)

Core/interface net traffic is collected and pre-analysis by the UTS

Centralized detection, analysis and alerts in the NDR (Network Threat Detection and Response)

Remote Security Assessment System (RSAS)

Regular assessment for the OS of the ATMAS & Tower ATMAS

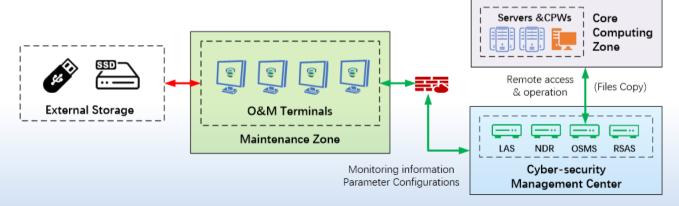




4

O&M terminals in the maintenance zone

- HMI for O&M staff to remotely access to servers and CPWs
- Authorized interface to external storage (including removable media)
- Control Monitor Display of the devices in cybersecurity center





- Security Private Network (SPN, Bypass)
 - X Net-N: Deployed in each ATMAS to transmit cyber-security related data
 - Net-M: Aggregate data from Net-N, and send to the cyber-security center
 - Terminal Access Point (TAP) : Aggregate and forward mirroring traffic from core/int net
- 6 Security Policies

- Service Minimization Socurity Polices
- Account & Permission Research Policy Management
- Software Adaptation

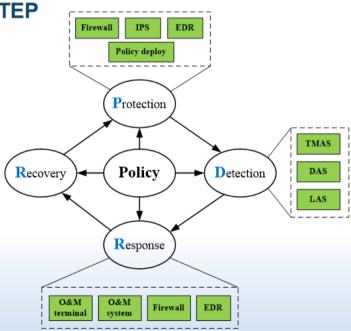




4 IMPLEMENTATION & NEXT STEP

System asset management & Security policy deployment (*Policy*)

- **Protection** with security devices
- Detection of threats occurred
- Response to security incidents
- System Recovery after threats clearance







FOCUS ON



Response to the ATMAS IGD

| KEY ELEMENT | Reference | Control measures | Conformity |
|---|---|---|------------|
| Cyber Security Policy | Establish the own Cyber Security Policy to mitigate cyber threat | Regulation and Standard for ATMAS have been established. Policies have been deployed with security devices | ✓ |
| Network Infrastructure Protection | FW/NIDS/NIPS to strengthen the protection for external TCP/IP communication | Deploy <u>FWs with IPS/AV</u> at the boundary of ATMAS to control external TCP/IP connection | |
| User Account Management | Establish systematic and traceable process for the administration of user accounts applicable | Deploy <u>O&M management system</u> to manage user accounts and authority, record O&M behavior for traceability | ⊘ |
| System Development Life Cycle | Protection from cyber threats throughout the system life cycle of ATMAS | Security devices have been implemented as an essential component in the <u>design</u> , <u>integration</u> , <u>acceptance</u> , and O&M of the ATMAS | |





FOCUS ON



Response to the ATMAS IGD

| KEY ELEMENT | Reference | Control measures | Conformity |
|--|---|---|------------|
| Removable Media Control | Removable media should be scanned by the machine prior to uploading data to ATMAS | O&M terminals to be provide as the authorized interface to connect removable media Removable media be scanned by EDR | ⊘ |
| Software Security Patch Management | Set up a scheme to work to evaluate system patches | RSAS to carry out regularly assessment for the ATMAS & Tower ATMAS | |
| Physical Security | Implement security measures to physically protect ATMAS | Physical protection measures (guards, CCTV, physical lock, etc.) have been implemented | |
| Response to Cyber Security Incidents | Exercises should be arranged to upkeep staff awareness and the robustness of the reporting mechanism. | Deploy <u>TMAS</u> , <u>DAS</u> and <u>LAS</u> to assist administrators/staffs in discovering and handling cyber security incidents | ⊘ |





FOCUS ON



Comparison of integrated solution and separate solution



System structure

Unified design Simplify the system structure Avoid duplication of similar devices



O&M can be done for the four system by devices in one security center Reducing training cost for staffs





Implementation

Deployment of security devices for four systems in one solution Difficulties in implementation

Investment

The one-time investment pressure brought by the amount of additional security devices







FOCUS ON



Devices list with recommended priority (L1 is the highest)

In considering of the system scale, investment budget, and the requirements of national cyber security policies

| Location | Device | Necessity | Priority | Suggestion |
|---------------------------|-----------------------|-----------|----------|---|
| System Boundary | Firewall | Essential | Level-1 | Implemented with ATMAS |
| | Data diode gateway | Optional | | Isolate connection to the areas with high risks |
| | DAS | Essential | Level-2 | Separate configure |
| Core Computing Zone | EDR | Recommend | Level-3 | Adaptation to ATMAS should be evaluated |
| | UTS | Recommend | Level-3 | Separate configure |
| | TAP | Optional | | |
| | LAS | Essential | Level-2 | Shared by muti-systems |
| Security | OSMS | Essential | Level-2 | Shared by muti-systems |
| Managem ent Zone | NDR | Recommend | Level-3 | Shared by muti-systems |
| | RSAS | Optional | | |
| O&M Zone | O&M terminal | Essential | Level-2 | Shared by muti-systems |
| SPN | Router Switch | Optional | | NET-S can be used as the security net |



FOCUS ON

- NAT to solve IP Confliction while multiple Systems Sharing Security Devices
- Personnel training to improve skills for cyber security O&M
- Virtualization technology (Resource Pool) to reduce the growth in the number of devices hardware

