

Design and Implementation of the Integrated Cybersecurity Solution for ATMAS and Tower ATMAS

(Presented by China)



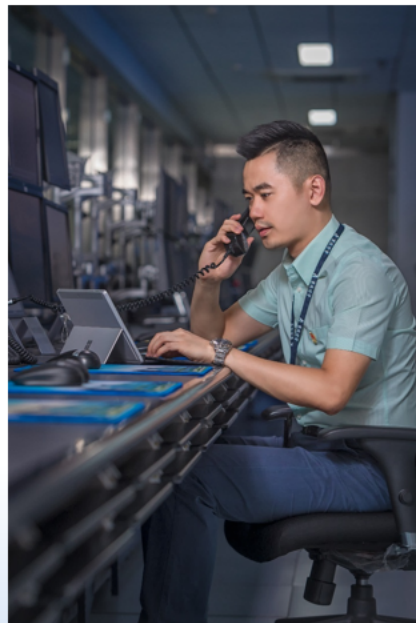


Biography of Mr. Gong Xinyu

*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

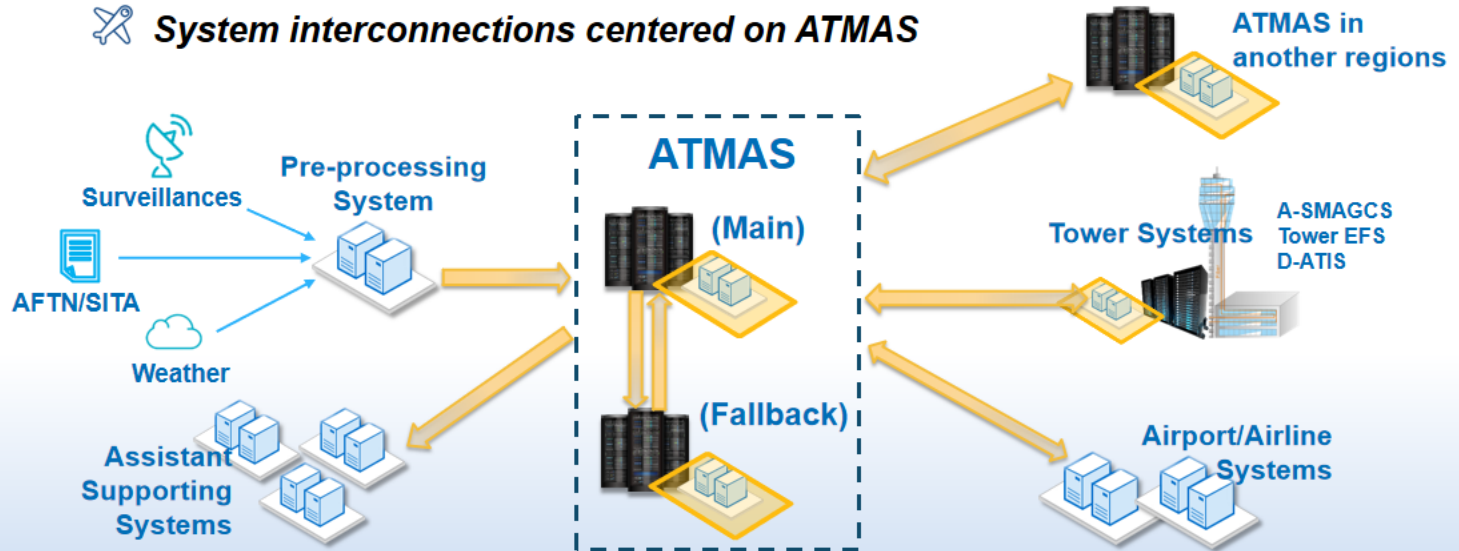
Part4: Implementation & Next step



1 BACKGROUND



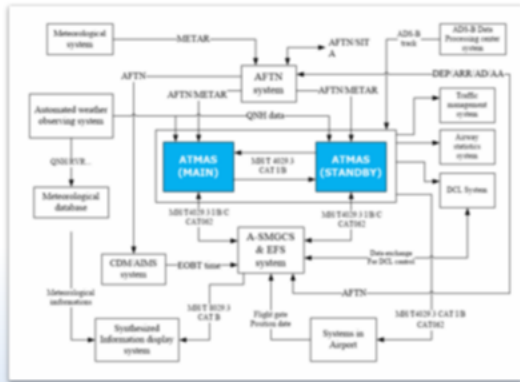
System interconnections centered on ATMAS



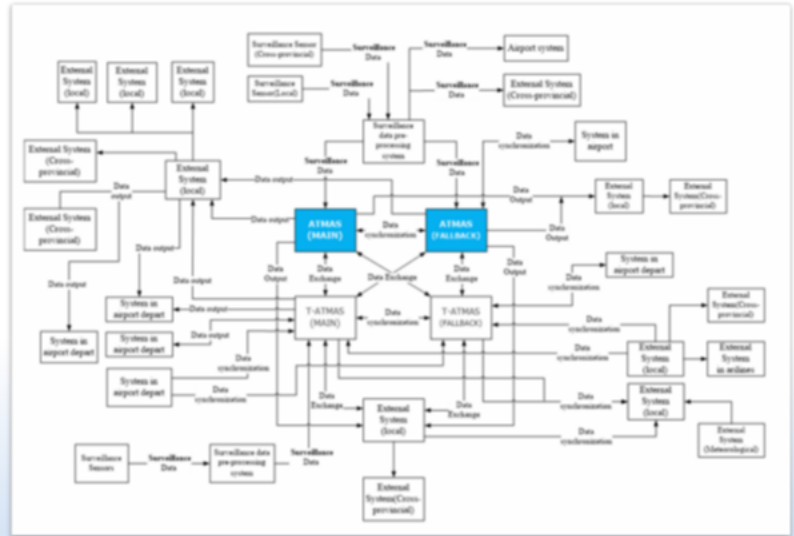


More external systems are connected to the ATMAS, ANSP have to face the increasing challenges in cyber security

System Interconnections in 2018

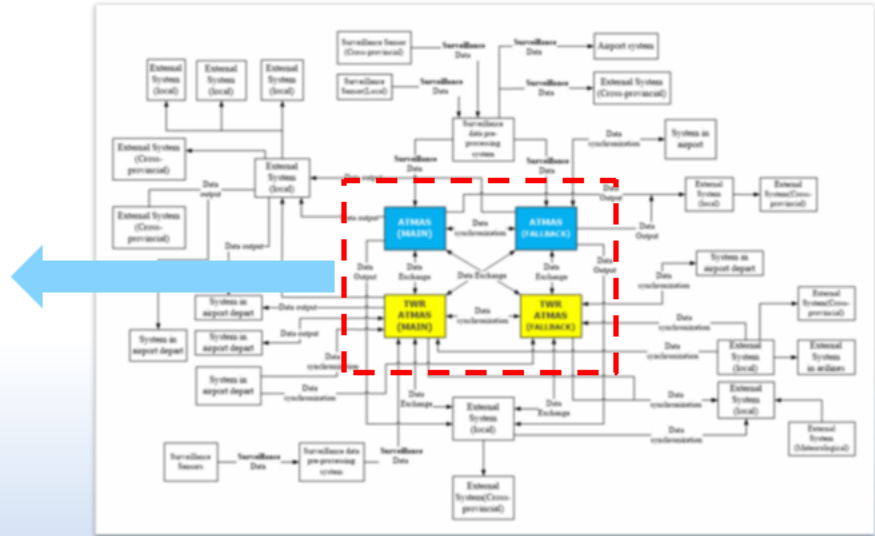
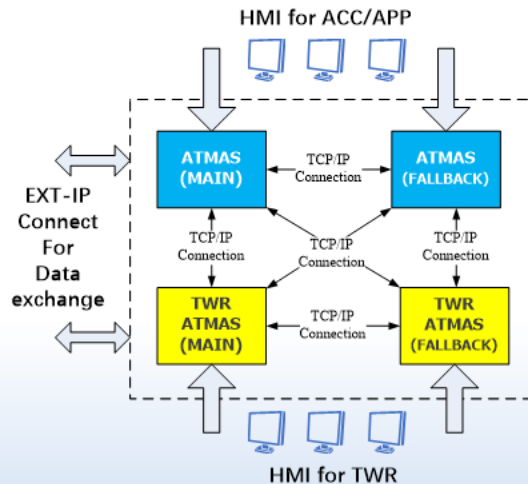


System Interconnections in 2024





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

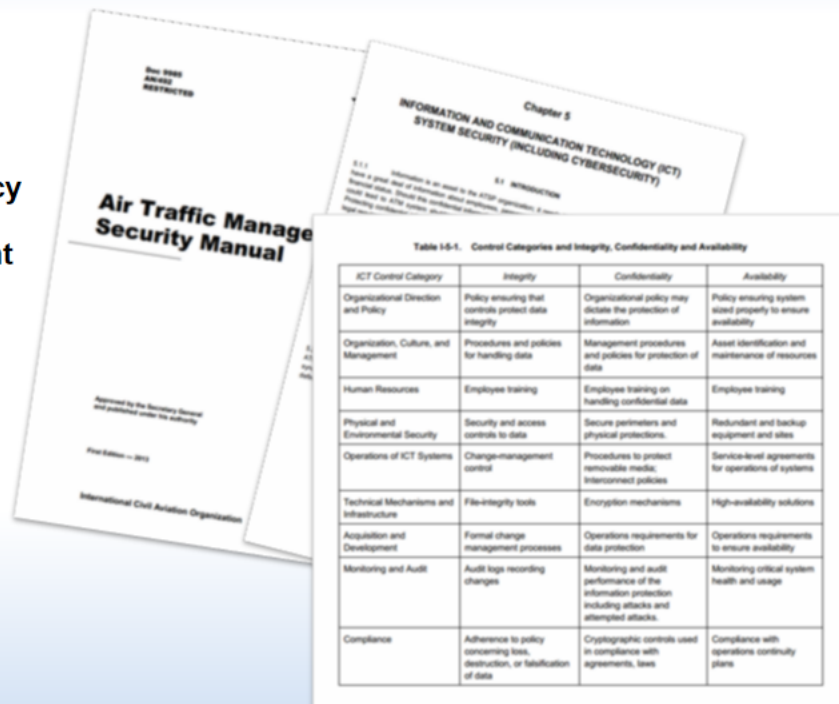




2 RESEARCH

Doc.9985

- 1 Organizational policy
- 2 Culture & Management
- 3 Human resources
- 4 Physical & Environmental
- 5 Operation
- 6 Technical infrastructure
- 7 Acquisition & Development
- 8 Monitoring & Audit
- 9 Compliance





1 Guidance by ICAO

ATMAS IGD

1 Cybersecurity Policy

2 Network Infrastructure

3 User Account Management

4 System Development Life Cycle

5 Removable Media Control

6 Software Security Patch Management

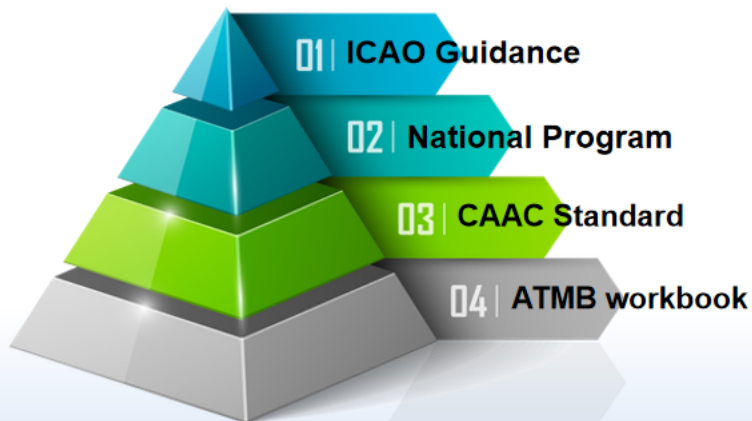
7 Physical Security Measures

8 Response to Cyber Security Incidents



2

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



**Baseline for
classified protection**



**Critical information
infrastructure protection**



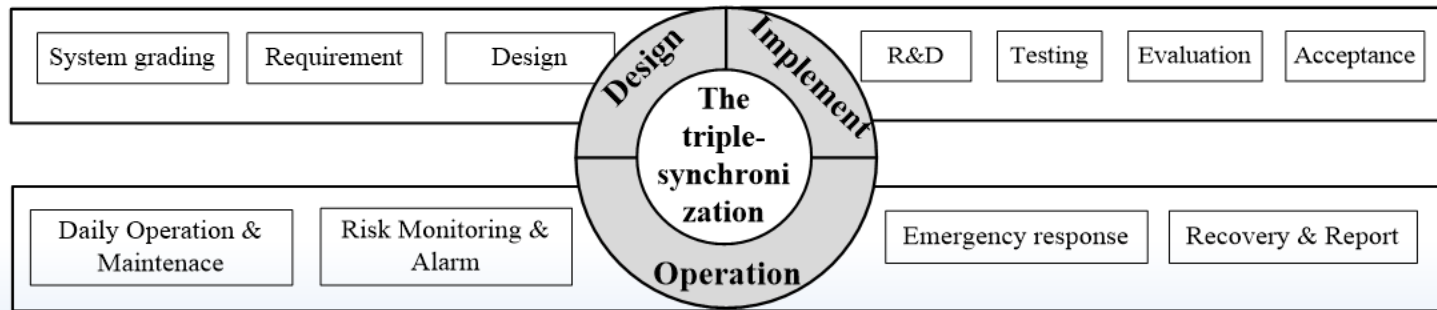
Since 2020, ATMB of CAAC has been working with equipment suppliers to carry out cybersecurity upgrades and evaluations of the ATMAS in multiple locations

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		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

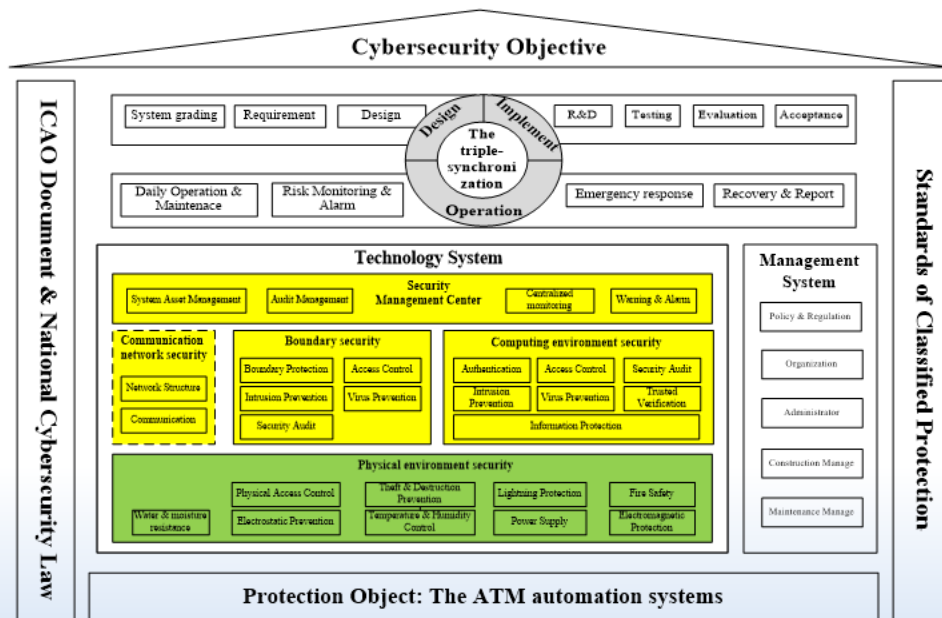




✈ The cybersecurity architecture for the ATMAS has been established


✈ Technology system is the foundation


One Center Triple Protections

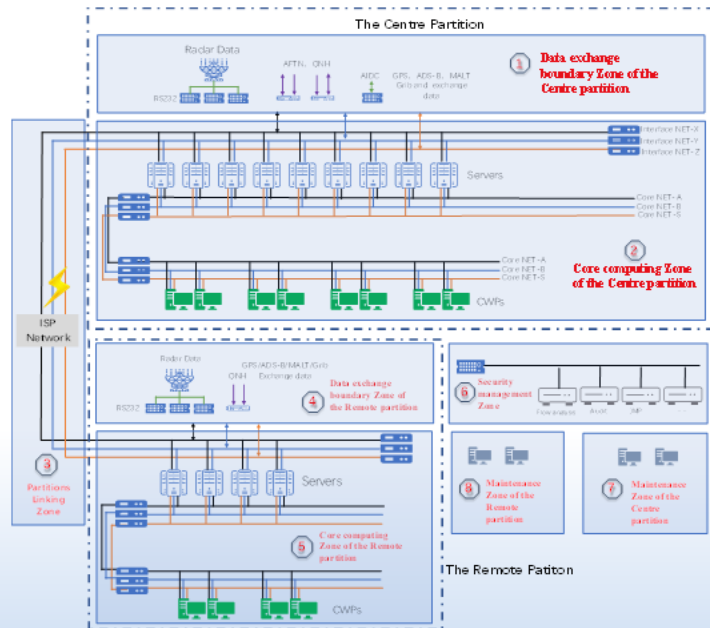
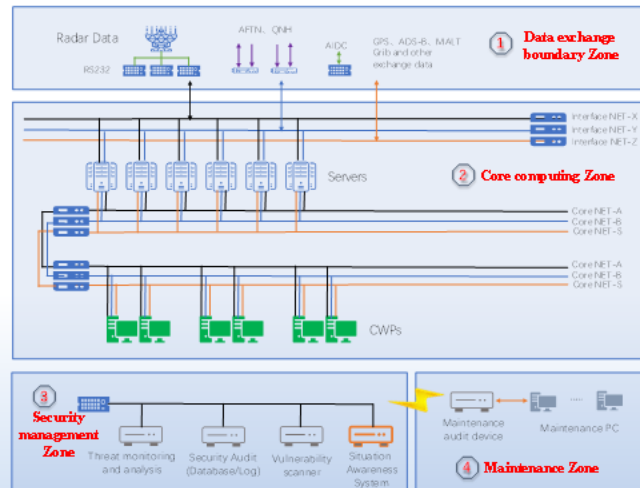


3

Technical Guidance for Classified Protection of Cybersecurity in ATMAS construction

 **Security Zone Division**

 **Devices configuration**



Design and implementation of the integrated cybersecurity solution for ATMAS and Tower ATMAS



3 SOLUTION



Design based on the Technical Guidance, in 2023



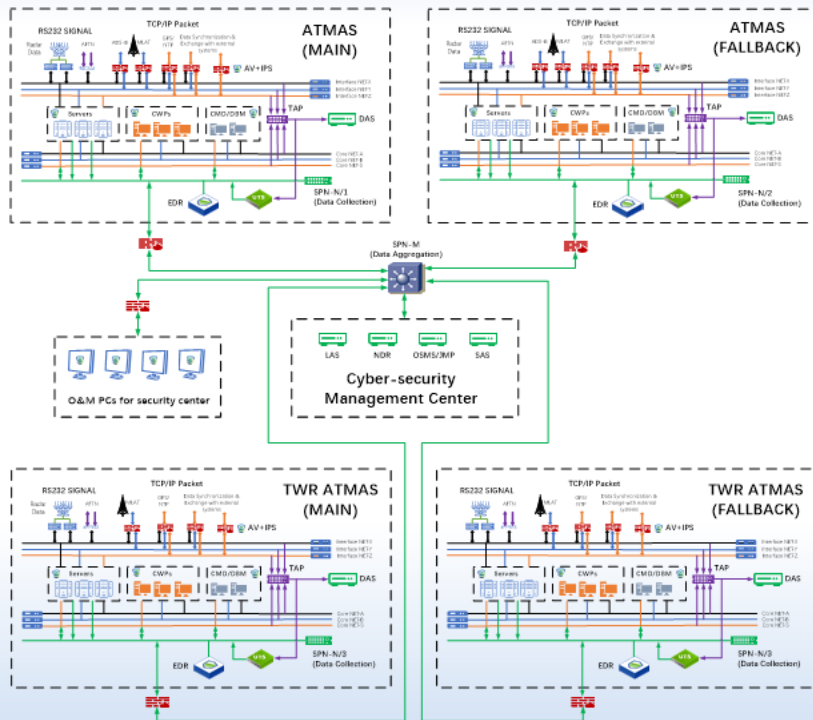
Integrated solution for ATMAS and Tower ATMAS considering the similarity of system topologies



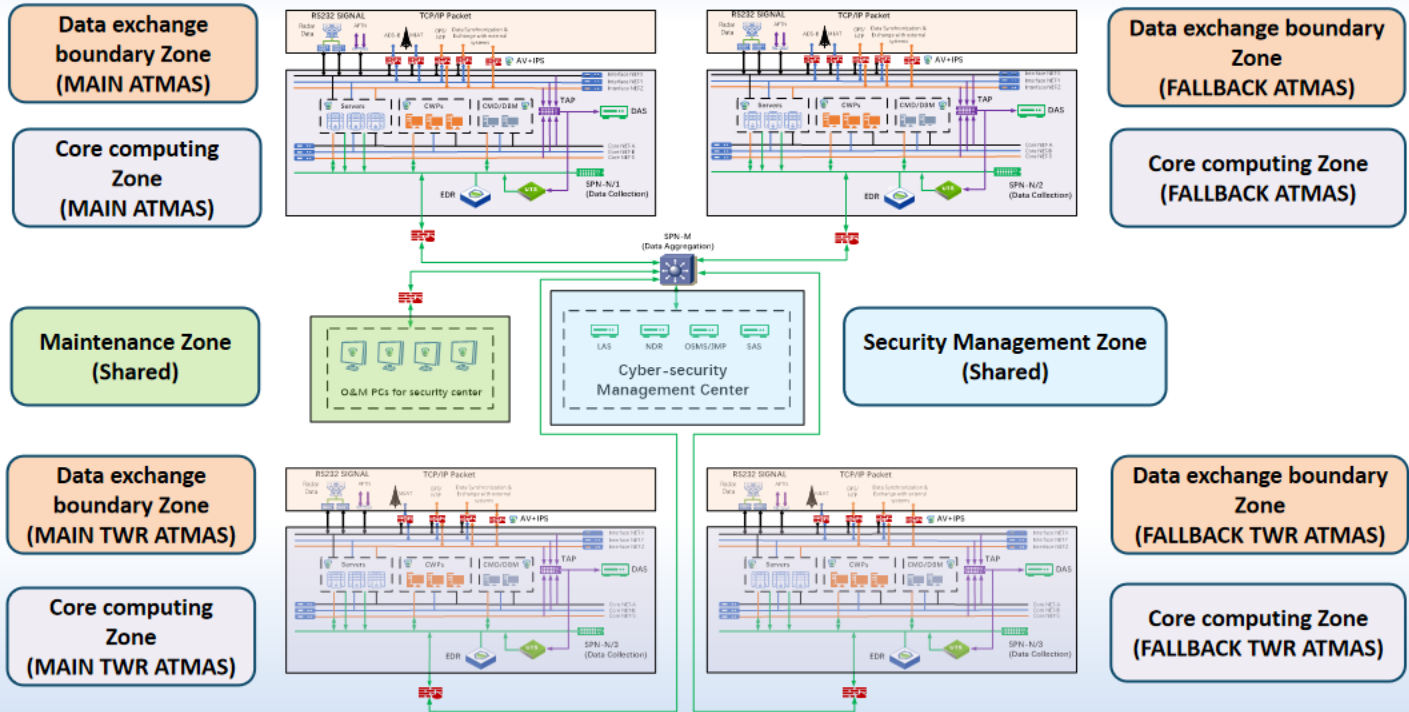
Applicable to ATMAS with only one partition



Being implemented in the Chongqing ATC center, in 2024



Design and implementation of the integrated cybersecurity solution for ATMAS and Tower ATMAS



1

Protection in the system boundary



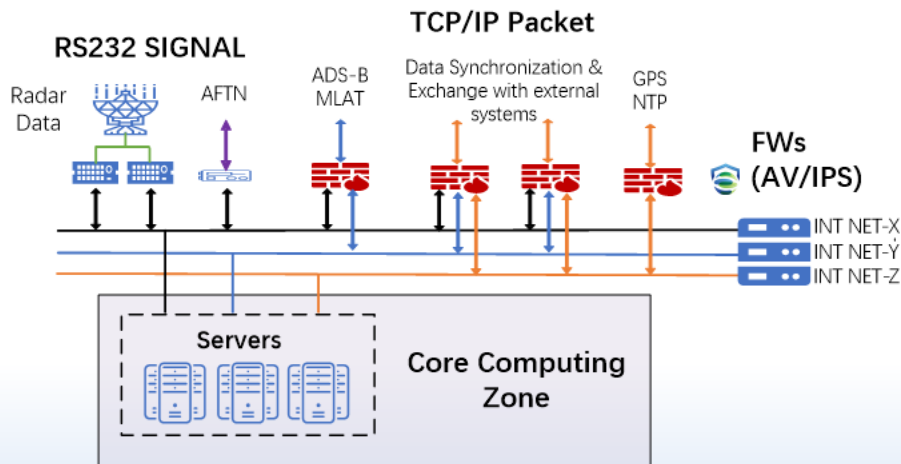
Firewalls (FWs)

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





2

Protections in the core computing zone



Database Audit System (DAS)

Alerts on unauthorized database access and data tampering

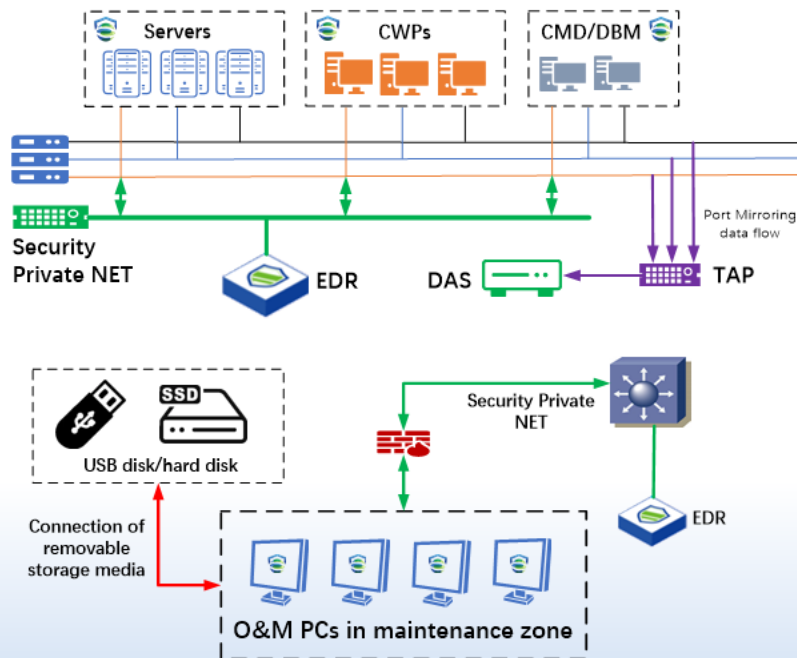


EDR Protection

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)

LOG Audit System (LAS)

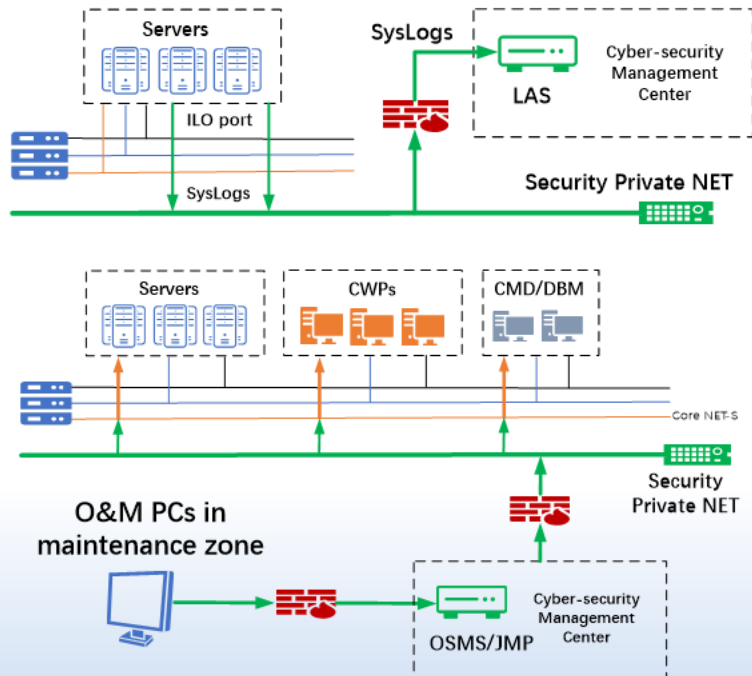
Collect system logs from servers
Alerts for abnormal log messages

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)

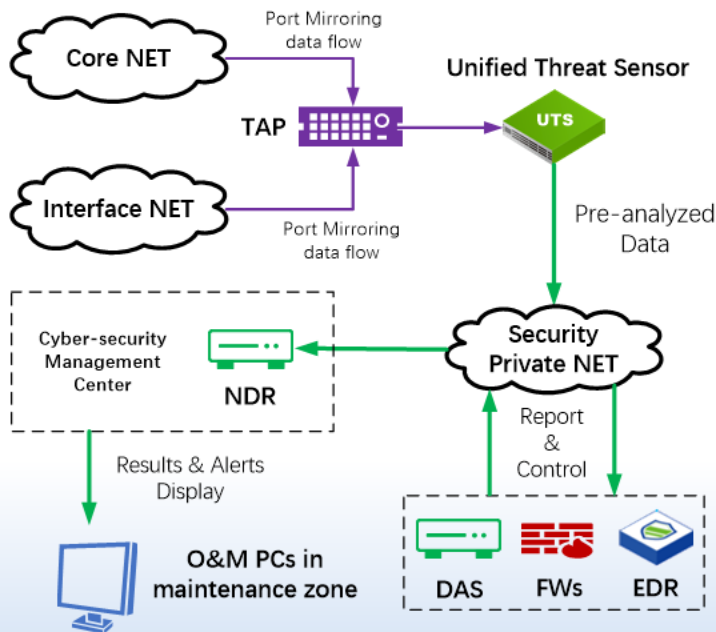
Core/interface net traffic is collected and pre-analysis by the UTS

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



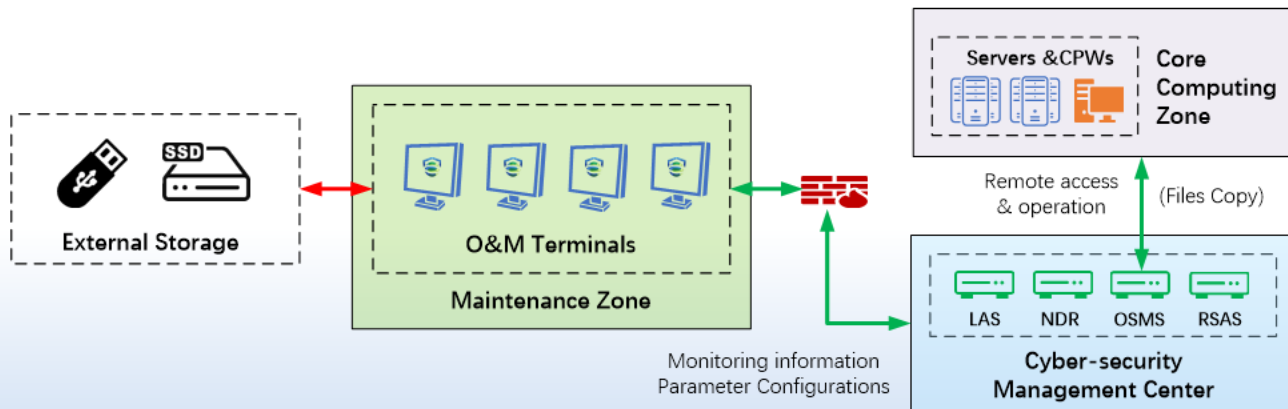
HMI for O&M staff to remotely access to servers and CPWs



Authorized interface to external storage (including removable media)






Control Monitor Display of the devices in cyber-security center











5 Security Private Network (**SPN**, Bypass)

-  **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


- | | | |
|--|---|--|
|  Policies in FW |  Service Minimization |  OS Security Polices |
|  Account & Permission Management |  Password Policy |  Software Adaptation |




4 IMPLEMENTATION & NEXT STEP

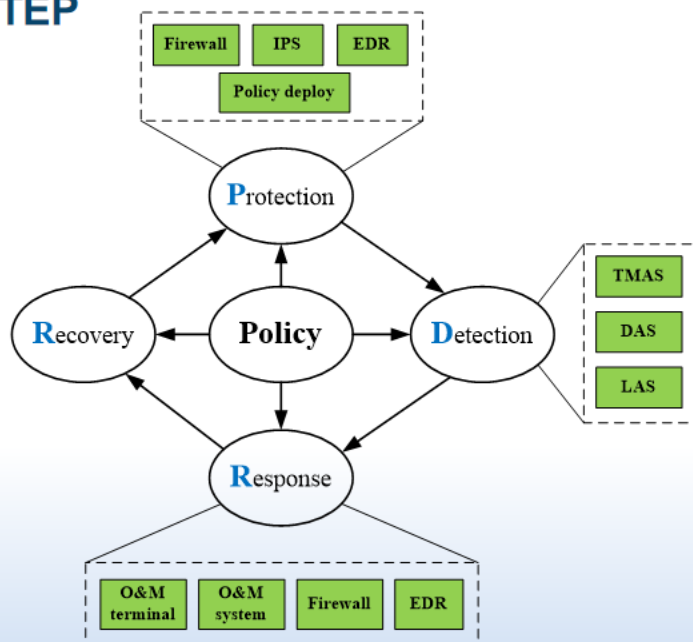
System asset management & Security
policy deployment (**Policy**)

 **Protection** with security devices

 **Detection** of threats occurred

 **Response** to security incidents

 **System Recovery** after threats
clearance





1

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	<u>Regulation and Standard</u> 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, integration, acceptance, and O&M</u> of the ATMAS	



1

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	<u>O&M terminals</u> to be provide as the authorized interface to connect removable media Removable media be scanned by <u>EDR</u>	
Software Security Patch Management	Set up a scheme to work to evaluate system patches	<u>RSAS</u> to carry out regularly assessment for the ATMAS & Tower ATMAS	
Physical Security	Implement security measures to physically protect ATMAS	Physical protection measures (<u>guards, CCTV, physical lock, etc.</u>) 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, DAS and LAS</u> to assist administrators/staffs in discovering and handling cyber security incidents	



1

FOCUS ON



Comparison of integrated solution and separate solution



System structure

Unified design
Simplify the system structure
Avoid duplication of similar
devices

Maintenance

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





1

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
Core Computing Zone	DAS	Essential	Level-2	Separate configure
	EDR	Recommend	Level-3	Adaptation to ATMAS should be evaluated
	UTS	Recommend	Level-3	Separate configure
	TAP	Optional	—	
Security Management Zone	LAS	Essential	Level-2	Shared by multi-systems
	OSMS	Essential	Level-2	Shared by multi-systems
	NDR	Recommend	Level-3	Shared by multi-systems
	RSAS	Optional	—	
O&M Zone	O&M terminal	Essential	Level-2	Shared by multi-systems
SPN	Router Switch	Optional	—	NET-S can be used as the security net



1

FOCUS ON



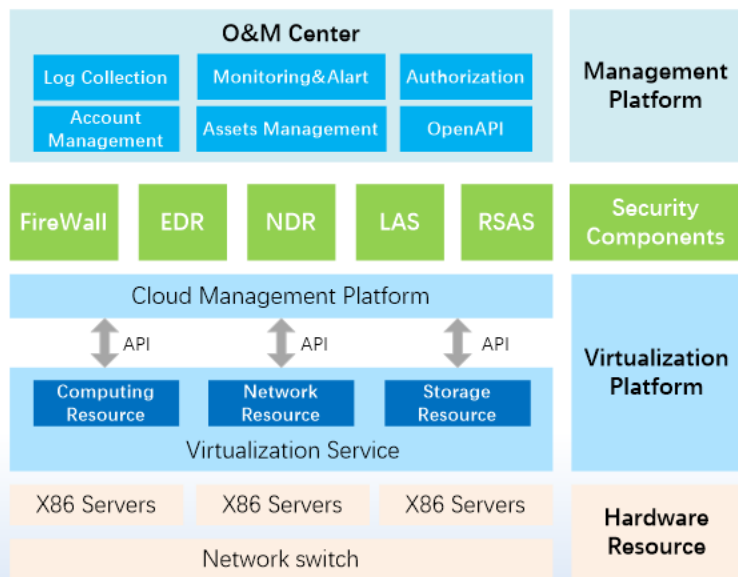
NAT to solve IP Confliction while multiple Systems Sharing Security Devices



Personnel training to improve skills for cyber security O&M



Virtualization technology (Resource Pool) to reduce the growth in the number of devices hardware





2

NEXT STEP



Cyber security Test Evaluation

Test evaluation plan based on the
features of ATMAS



Adaptation of commercial products and ATMAS

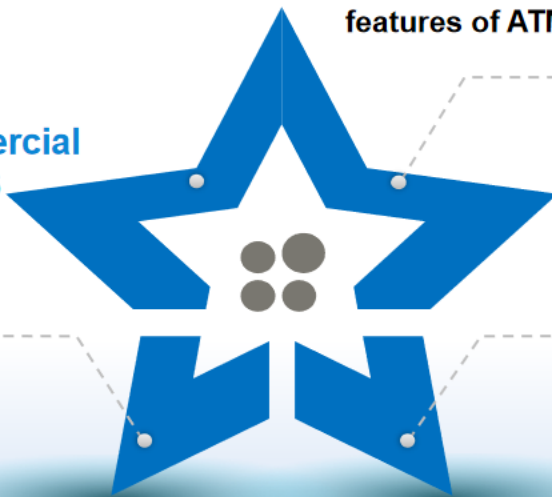
Lightweight EDR to minimize
the resource usage

API specification for different
brands of security device



Solution for ATMAS with multi-partitions

Research of integrated
solution for ATMAS and
TWR-ATMAS with multi-
partitions





中国民用航空局
空中交通管理局
Air Traffic Management Bureau .CAAC

Thank You!

