南京莱斯信息技术股份有限公司
Nanjing LES Information Technology Co., Ltd

Risk-based assessment and enhancement on management of Cyber Security Threats for ATM Automation System

ICAO, China,November 2018

Contents

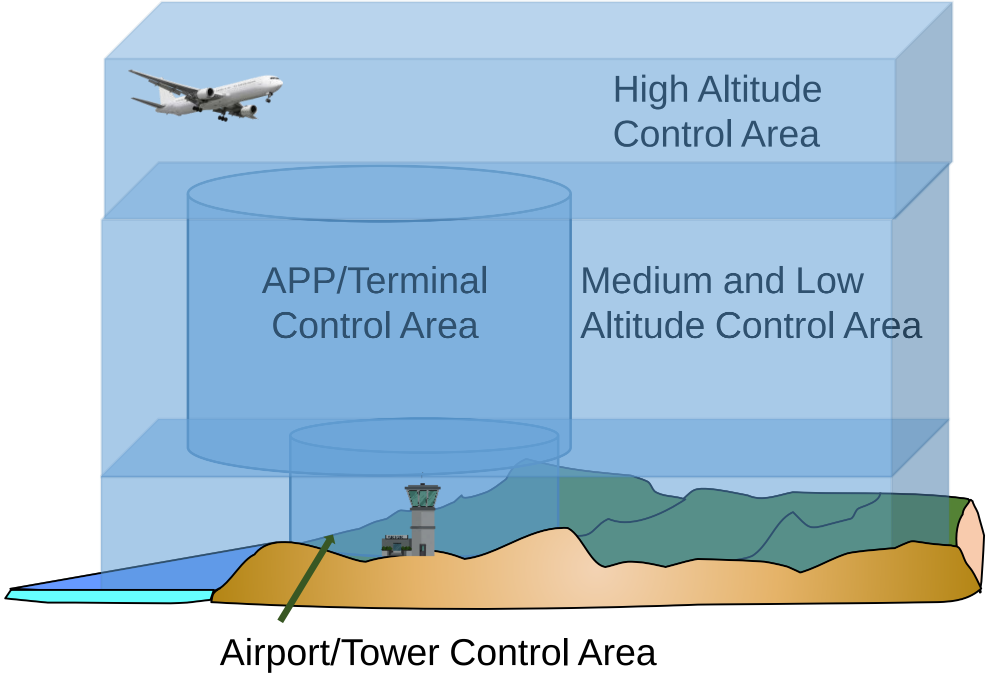
1 Current ATM Automation System Structure and Its Security

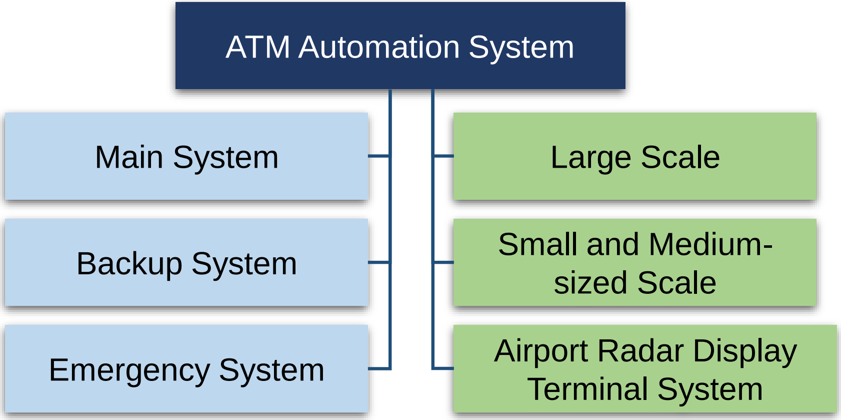
2 Risk Assessment Method and Flow

3 Assessment Case Briefing

1. Current ATM Automation System Structure and Its Security

Current ATM Automation System Structure

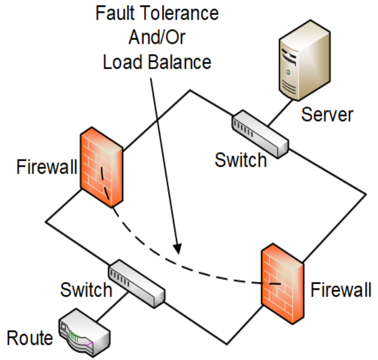

High Altitude Control Area
APP/Terminal Control Area
Medium and Low Altitude Control Area
Airport/Tower Control Area



- **Multilevel : ACC, APP and TWR**
- **Classified with different types on ATC Automation system function and its scale**

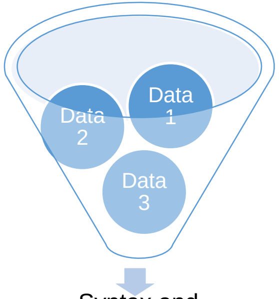
1. Current ATM Automation System Structure and Its Security

Common Security Solutions



Optimization of Data Input

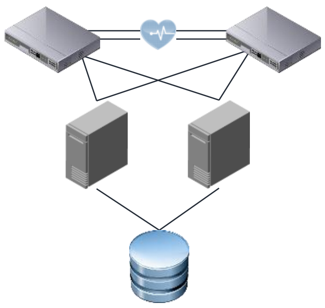
- Dual-channel data access
- Radar signal optimization



Syntax and Semantics Check

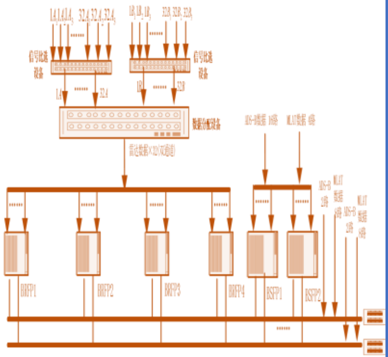
Redundant System Network

Three redundant LANs are applied, and the service LAN is configured on different PhysX card.



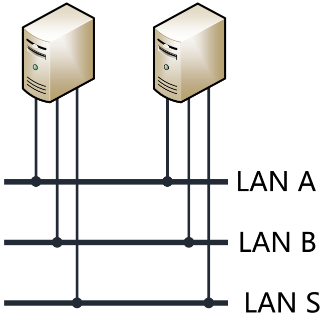
Firewall Security

Security isolation between systems by firewalls.



Data Input Validation

Syntax and Semantics Check on data input.



System Equipment Redundancy

Adopts the redundancy config. to enhance the ability to prevent the single point of failure.

1. Current ATM Automation System Structure and Its Security

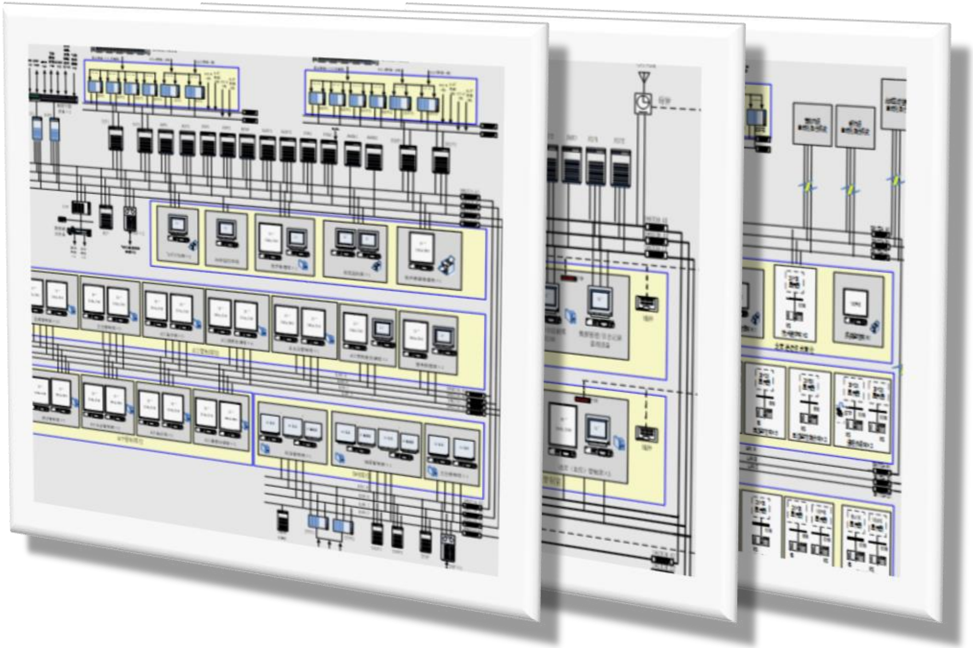
- **The main characteristics of the System structure are:**

Intranet Private Network

Physically isolated with the Internet

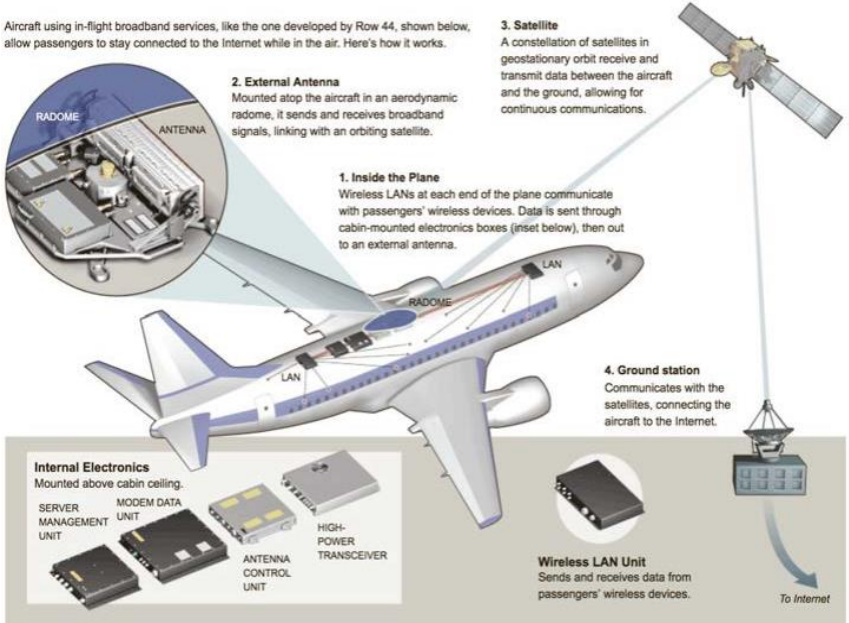
DPLC connections with different systems

Data input method:RS232 and IP



1. Current ATM Automation System Structure and Its Security

Growing cyber-risks are rising questions to many ATC Systems



Aircraft using in-flight broadband services, like the one developed by Row 44, shown below, allow passengers to stay connected to the Internet while in the air. Here's how it works.

1. Inside the Plane
Wireless LANs at each end of the plane communicate with passengers' wireless devices. Data is sent through cabin-mounted electronics boxes (inset below), then out to an external antenna.

2. External Antenna
Mounted atop the aircraft in an aerodynamic radome, it sends and receives broadband signals, linking with an orbiting satellite.

3. Satellite
A constellation of satellites in geostationary orbit receive and transmit data between the aircraft and the ground, allowing for continuous communications.

4. Ground station
Communicates with the satellites, connecting the aircraft to the Internet.

Internal Electronics
Mounted above cabin ceiling.

Wireless LAN Unit
Sends and receives data from passengers' wireless devices.

Hackers could even bring down a plane through on-board entertainment systems

Pic. Cited: Last Call for SATCOM Security, Ruben Santamarta, IOActive, Aug.2018

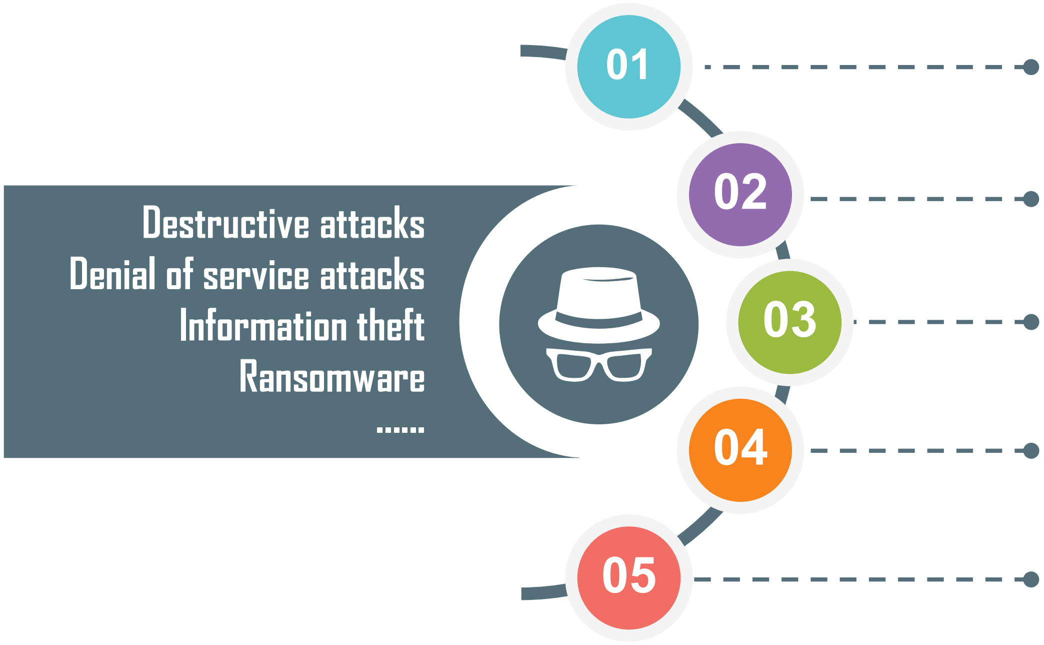
ATC systems are vulnerable to cyberattack

- Hackers may gain access to personally identifiable information(e.g. social security numbers, private informations of employees, etc.) via public-facing network.

- It is possible to forge the ADS-B broadcast packet with a man-in-the-middle (MitM) attack, e.g. a threat actor could take a plane and make it appear miles away from its actual location.

1. Current ATM Automation System Structure and Its Security

Growing cyber-risks are rising questions to many ATC Systems



Destructive attacks
Denial of service attacks
Information theft
Ransomware
……

01 How to cope with strengthening regulation for legacy systems?

02 Is my surveillance network a major weakness?

03 Does cyber-protection enough?

04 Does contingency planning enough?

05 What is the safety and operational impacts of cyber-attacks?

Contents

1 Current ATM Automation System Structure and Its Security

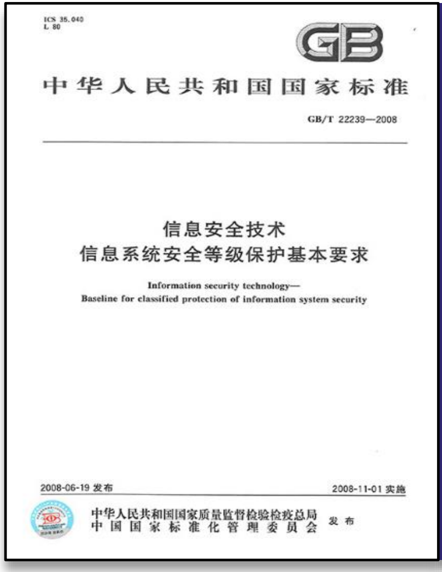
2 Risk Assessment Method and Flow

3 Assessment Case Briefing

2. Risk Assessment Method and Flow

Assessment Basis

- 《Air Traffic Management Security Manual》(ICAO Doc 9985-AN/492)
- 《Information security technology-Implementation guide for classified protection of information system》(GB/T 22239-2008)
- 《Information technology-Security techniques-Information security management systems-Requirements》(ISO/IEC 27001)
- 《Information technology-Security techniques-Code of Practice for Information security management》(ISO/IEC 27002)



ICS 35.040
L 80

GB

中华人民共和国国家标准

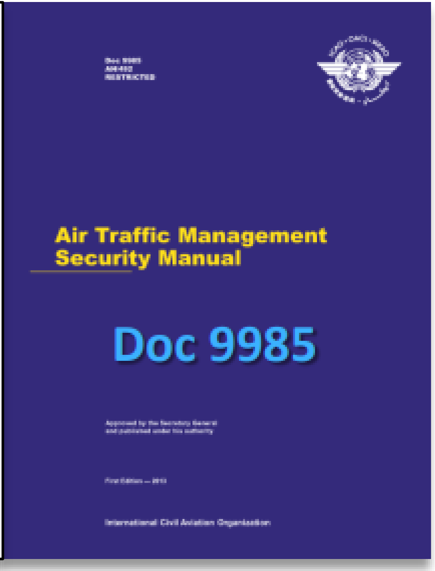
GB/T 22239—2008

信息安全技术
信息系统安全等级保护基本要求

Information security technology—
Baseline for classified protection of information system security

2008-06-19 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布



Doc 9985
AN/492
RESTRICTED

Air Traffic Management
Security Manual

Doc 9985

Approved by the Secretary General
and published under his authority

First Edition — [illegible]

International Civil Aviation Organization

2. Risk Assessment Method and Flow

Main Tasks of Assessment

Identify Potential Risk

To identify the faced risks of the object

Assess Negative Effect

To assess the risk probability and negative effect

Confirm Bearing Capacity

To confirm the bearing capacity of the organization

Classify Priority Level

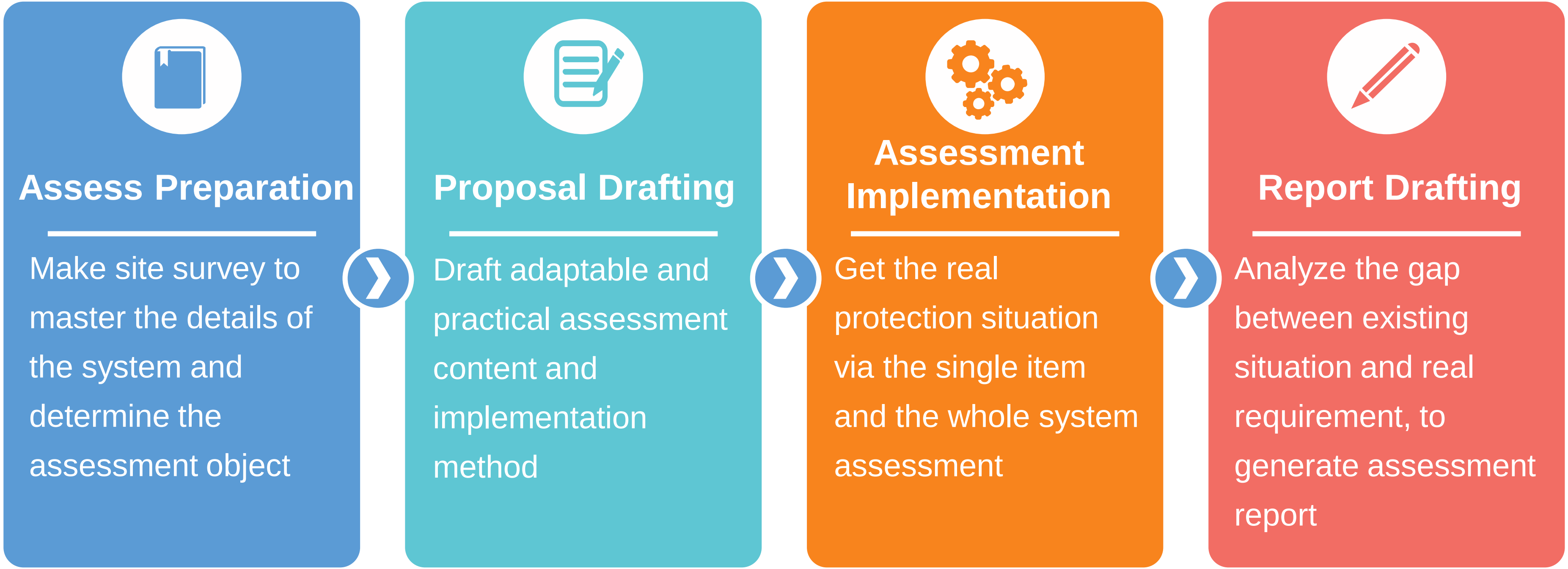
To classify the risk mitigation and control priority

Propose Mitigation Solution

To propose risk mitigation solution

2. Risk Assessment Method and Flow

■ Assessment Process



Assess Preparation

Make site survey to master the details of the system and determine the assessment object

Proposal Drafting

Draft adaptable and practical assessment content and implementation method

Assessment Implementation

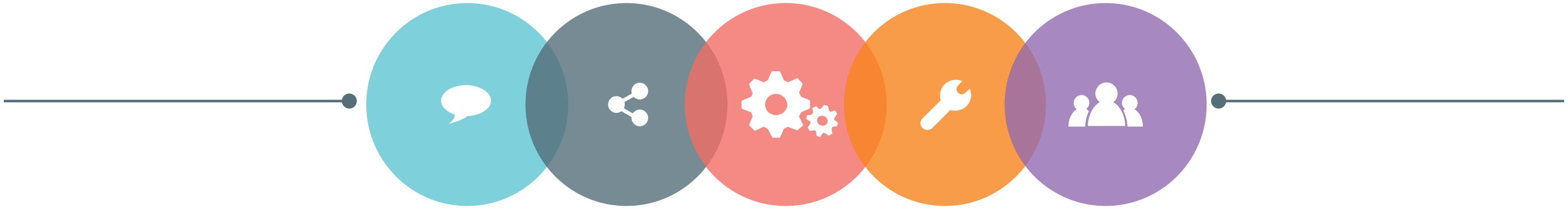
Get the real protection situation via the single item and the whole system assessment

Report Drafting

Analyze the gap between existing situation and real requirement, to generate assessment report

2. Risk Assessment Method and Flow

Implementation Method



01 Interview

To get the proof and related information by communication and discussion

02 Document Review

- ✓ To check the completeness of document
- ✓ To check the regulation implementation record
- ✓ To check the integrity and consistency of the above mentioned files

03 Configuration Check

To test the correctness of the configuration and verify the document content

04 Tool Test

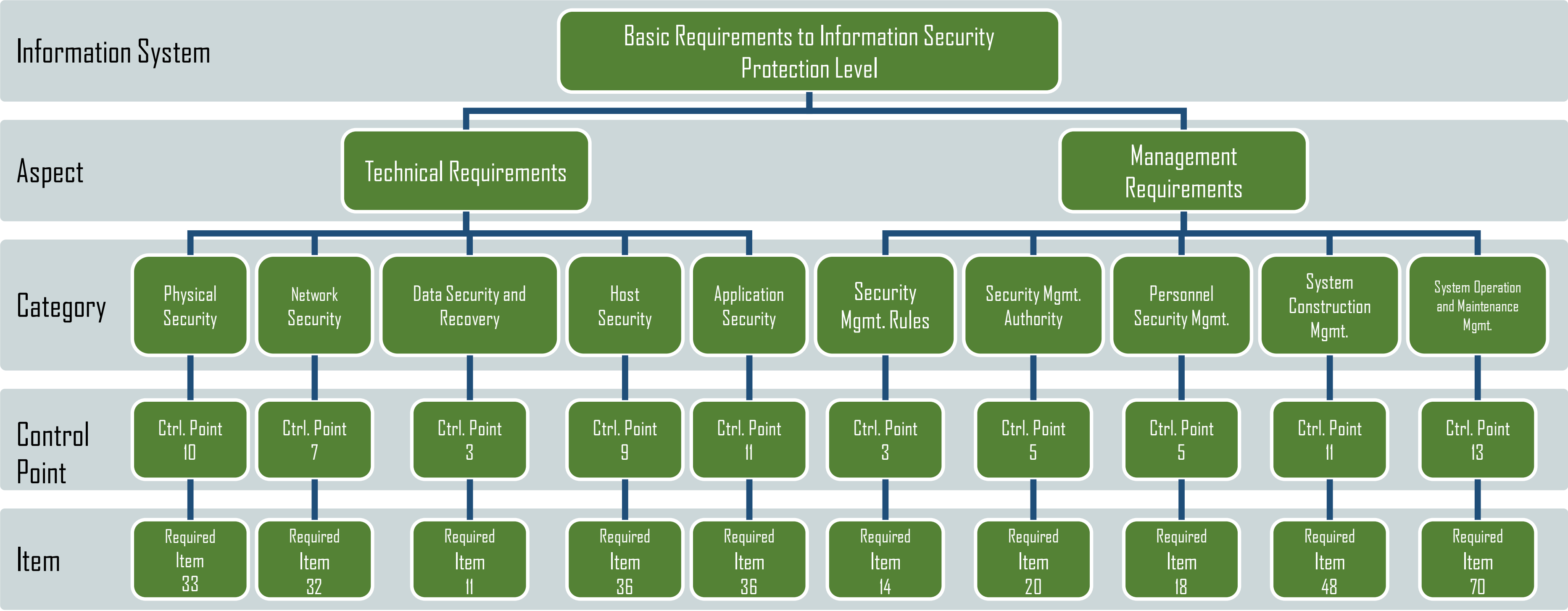
According to the test instruction manual, to make test to the system via the technical tool

05 Site Survey

To make site survey, in order to test if it meets the corresponding security level requirements

2. Risk Assessment Method and Flow

Assessment Related Specification



Information System: Basic Requirements to Information Security Protection Level

Aspect: Technical Requirements; Management Requirements

Category	Control Point	Item
Physical Security	Ctrl. Point 10	Required Item 33
Network Security	Ctrl. Point 7	Required Item 32
Data Security and Recovery	Ctrl. Point 3	Required Item 11
Host Security	Ctrl. Point 9	Required Item 36
Application Security	Ctrl. Point 11	Required Item 36
Security Mgmt. Rules	Ctrl. Point 3	Required Item 14
Security Mgmt. Authority	Ctrl. Point 5	Required Item 20
Personnel Security Mgmt.	Ctrl. Point 5	Required Item 18
System Construction Mgmt.	Ctrl. Point 11	Required Item 48
System Operation and Maintenance Mgmt.	Ctrl. Point 13	Required Item 70

Contents

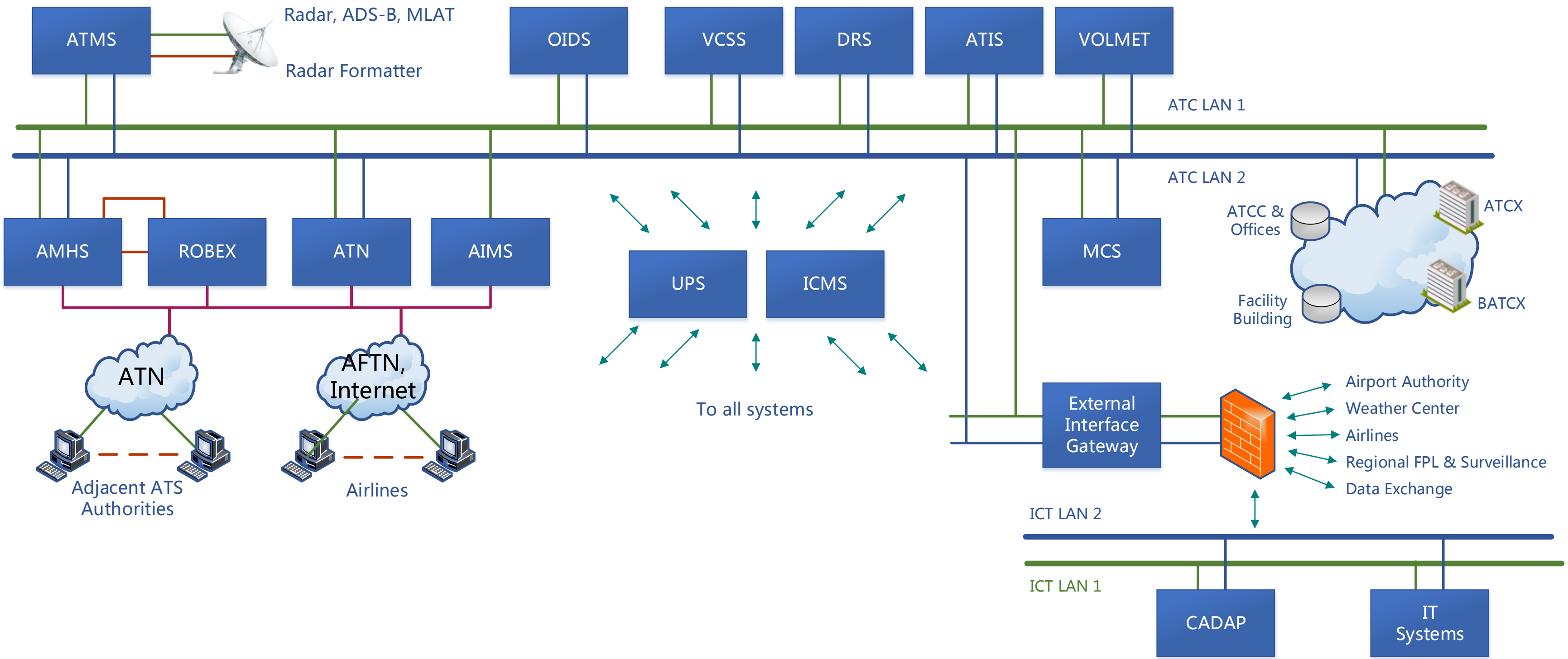
1 Current ATM Automation System Structure and Its Security

2 Risk Assessment Method and Flow

3 Assessment Case Briefing

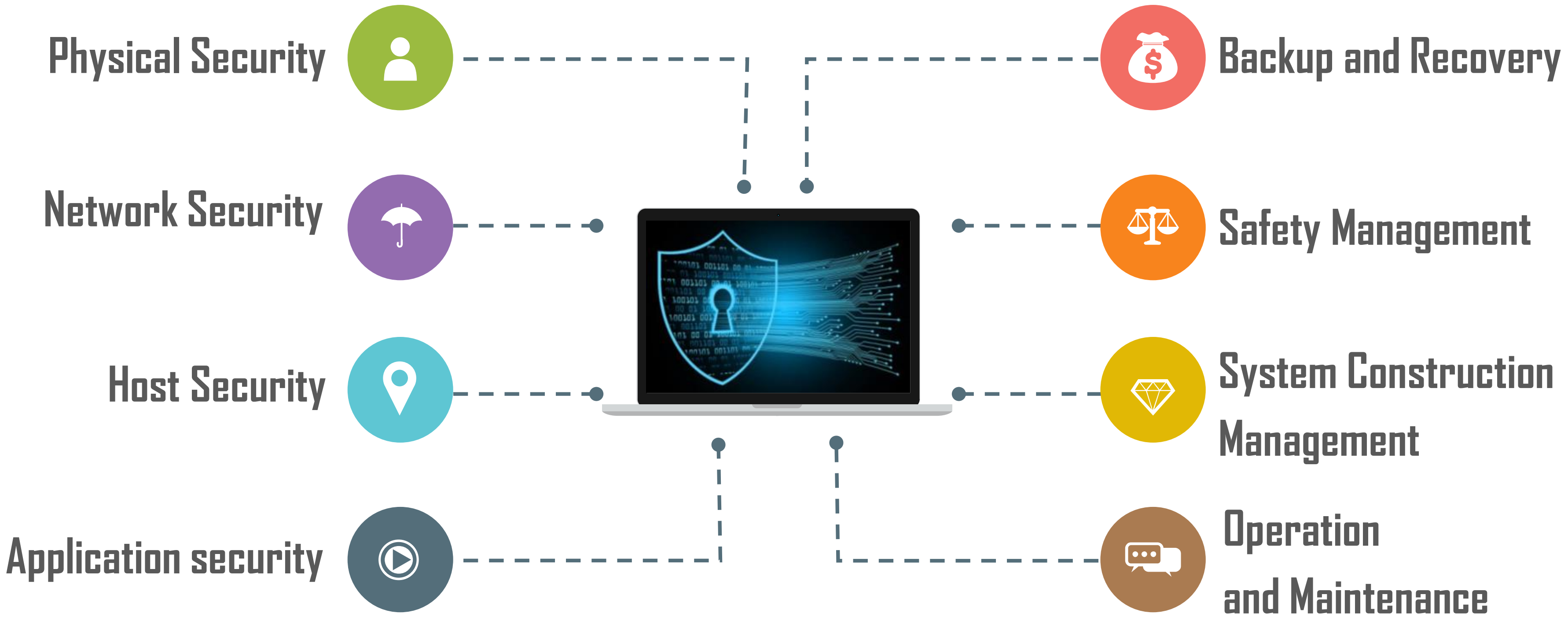
3. Assessment Case Briefing

Assessment Related Specification



3. Assessment Case Briefing

■ Scope



3. Assessment Case Briefing

Method

- Determine basic indicators
- Select evaluation object
- Eliminate inapplicable indicators
- Risk analysis

Physical security		
evaluation object	coincidence	Safety control point

Cyber security								
evaluation object	coincidence	Safety control point						
		frameworks security	Network Access	Security Auditing	Perimeter defense	intrusion prevention	Malicious Code	facility preserving
Network devices	High grade	7	5	12	2	2	0	21
	qualified	0	0	0	0	0	0	0
	disqualification	0	0	0	0	0	0	0
	Not Applicable	0	3	0	0	0	2	3

3. Assessment Case Briefing

- More Interconnected systems means more reachable targets

1 Increasing Connectivity and use of non-protected by design A/G Data Link Communication

2 More access points with networking and System Wide Information Management(SWIM) for CDM

3 Migration for interoperability to standard IP-based network with publicly available vulnerabilities

4 Less isolated architectures with clouded sevices, virtual center, total airport management...

3. Assessment Case Briefing

Summary

- With the continued growth in cyber security threats, both from inside and outside of an ANSP. The ICAO Doc 9985 ATM Security Manual is relevant .

- Proactive steps should be taken, including risk mitigation during system planning and design stage; physical, system and human provisions, etc..

- It is a good practice to consider conducting a third party cyber security audit to the ATM system and operations.

Thank you for your attention!

He Liang
Nanjing LES Information Technology Co., Ltd
Tel No.: +86 (0)25 8228 5124
Email: he_liang@les.cn

CETC 中国电科

责任 创新 卓越 共享 Responsibility Innovation Excellence Shared