ICAO

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

RISKS OF ATM AUTOMATION SYSTEM REGARDING INTERCONNECTION ENVIRONMENT

GongXinyu
SWATBM

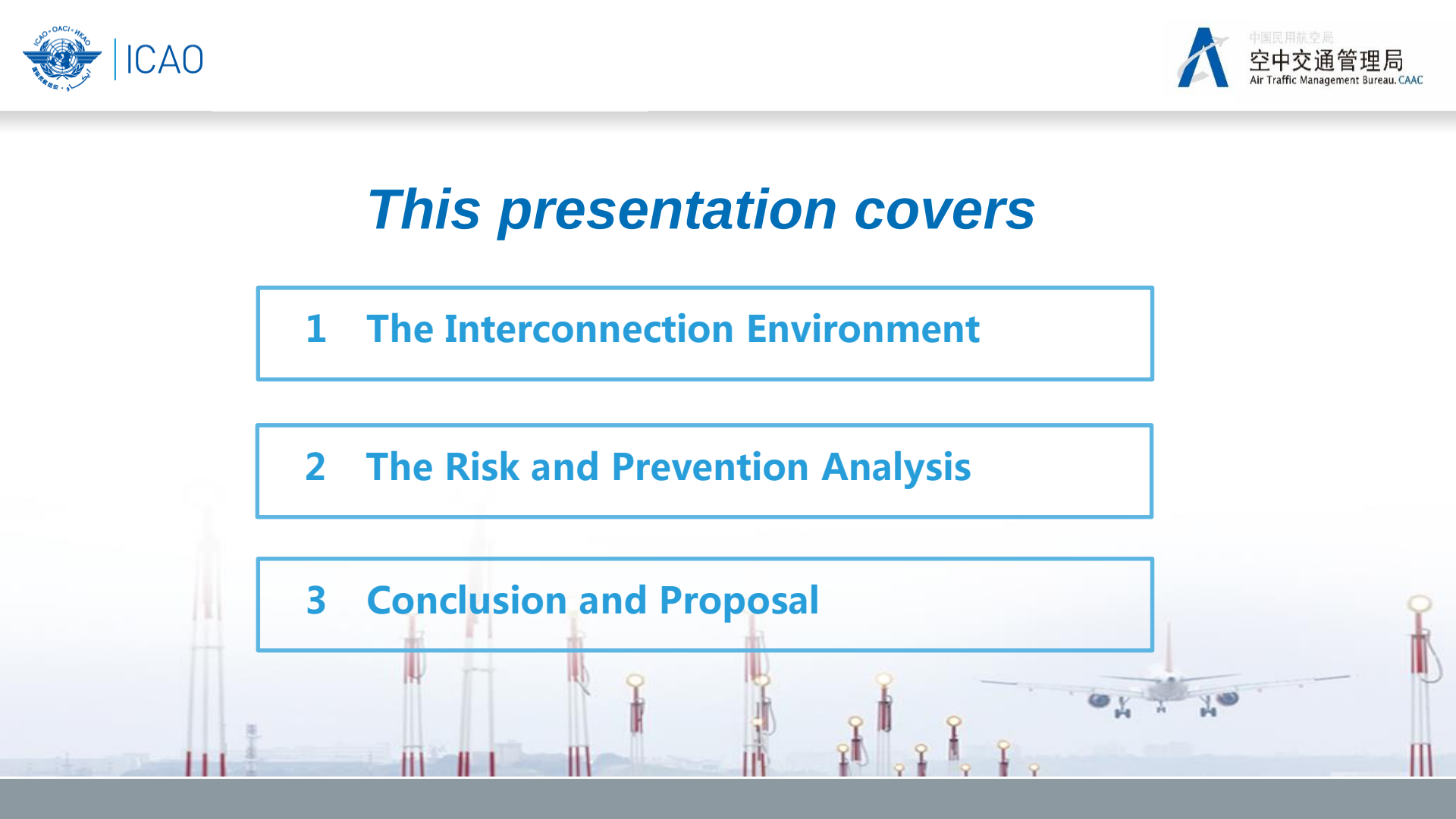
Nanjing, China 2018.11.22

This presentation covers

1 The Interconnection Environment

2 The Risk and Prevention Analysis

3 Conclusion and Proposal

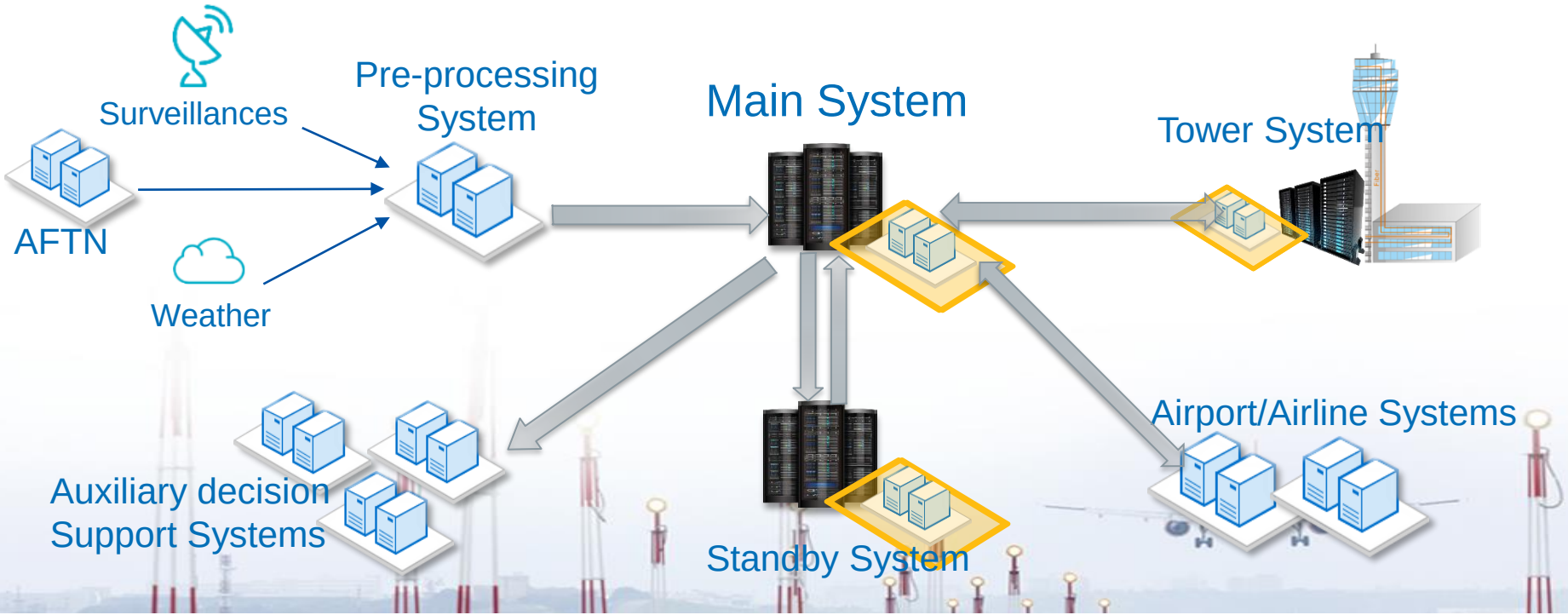


Interconnection Environment

- ***ATM automation system is the core human-machine interface (HMI) for controllers***
- ***The operational data has a high application value***
  - Accurate
  - Real-time
  - Predictive
  - Be manually verified and corrected

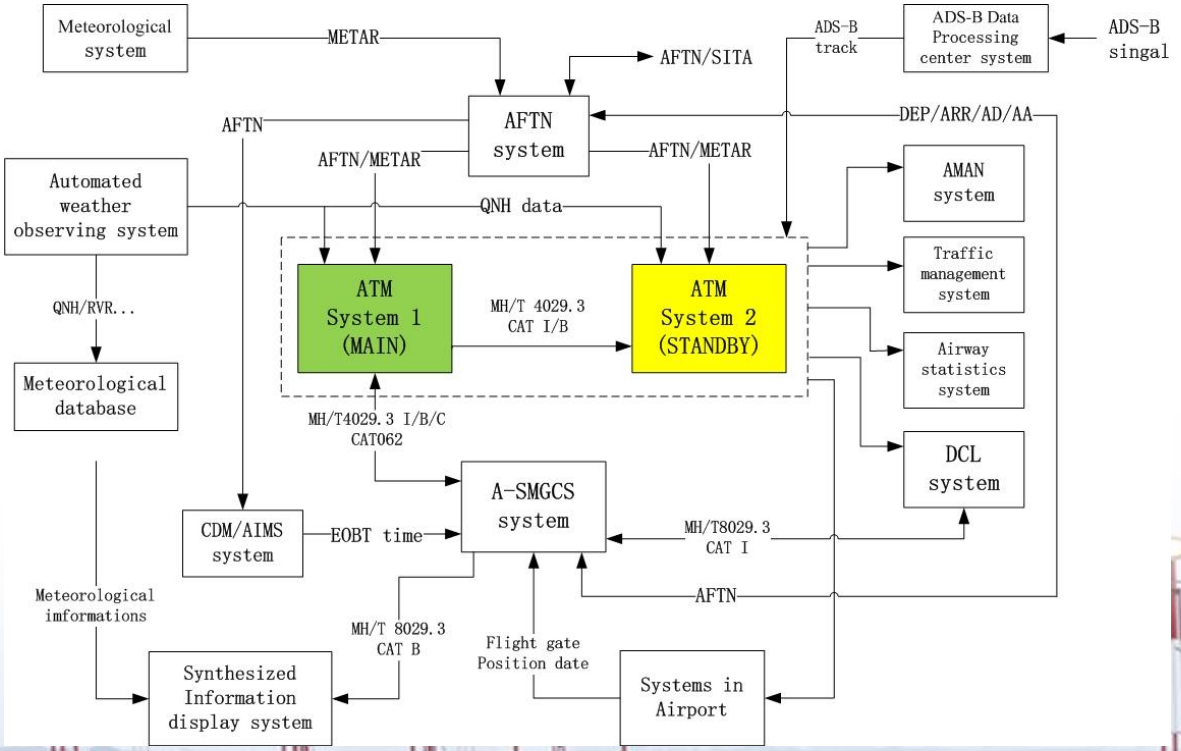
- ***Research and experiment on technical standards***
  - MH/T 4029.3
  - E-FEED
  - ADEXP
  - CAT062
  - MH/T 4008
  - Private interface

System interconnections by the core of ATM automation system



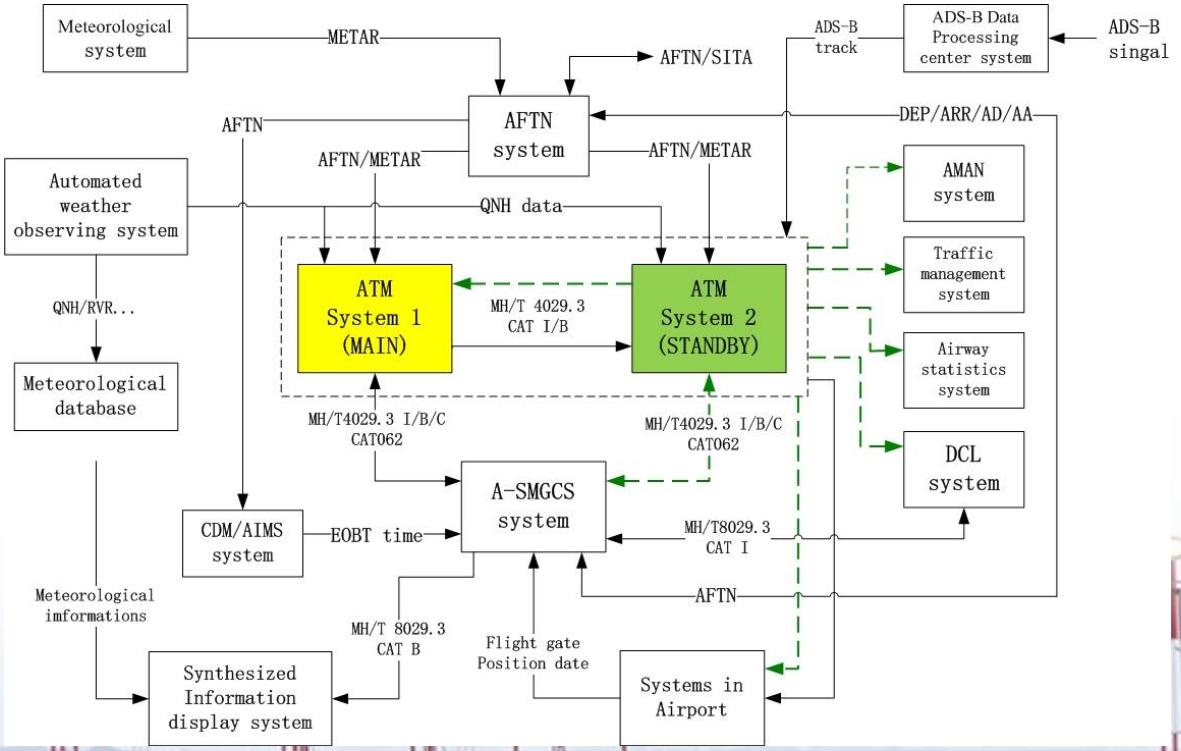
Interconnection Environment

- The system interconnection structure in the Chongqing ATC center



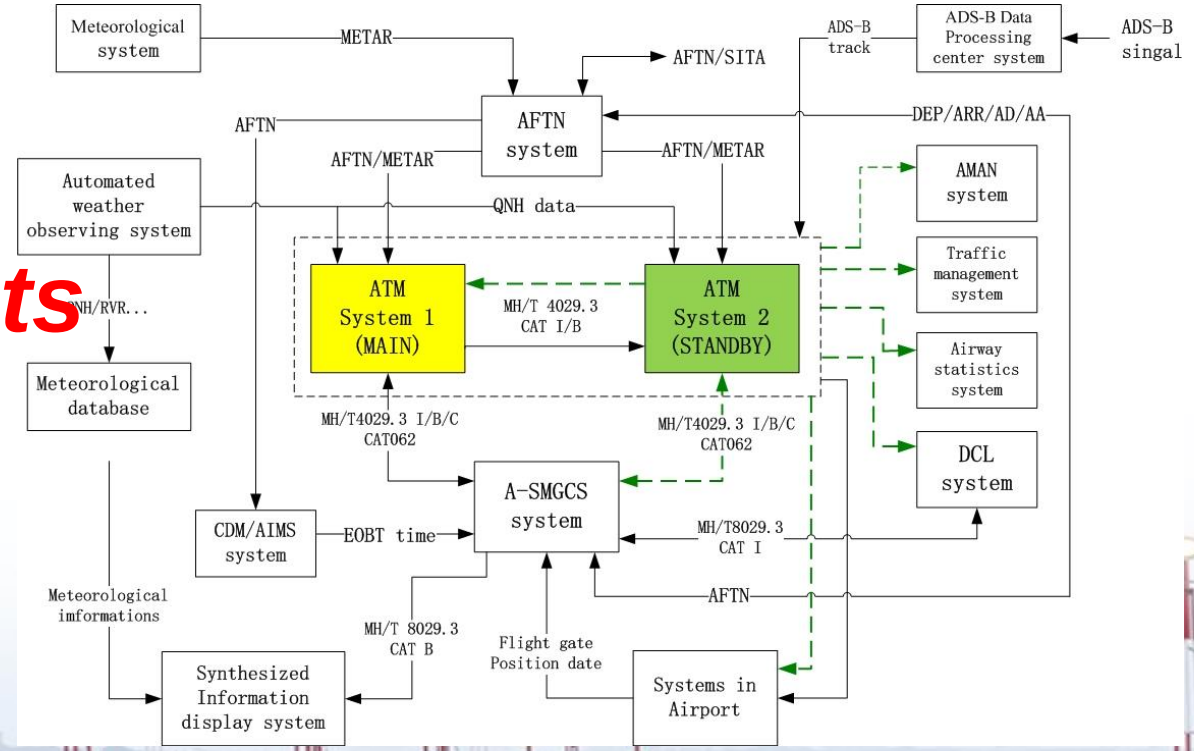
Interconnection Environment

- Standby automation system is required to be able to establish data links with all the peripheral systems



Interconnection Environment

Potential Risks & Threats



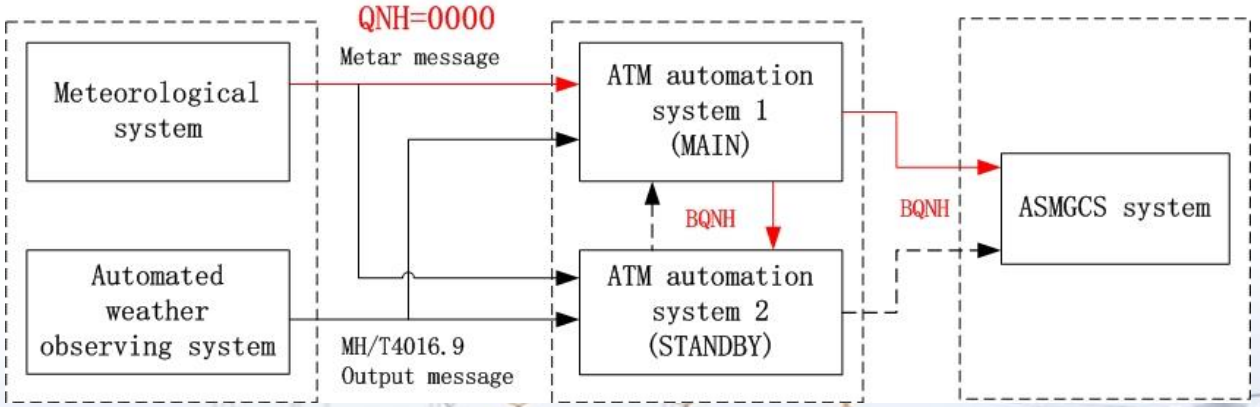
Risk Analysis & Prevention Suggestion

- ***Focus on risks from the following aspects***
  - The risk of multiple system failures caused by input data or signal
  - Flight plan processing failure caused by the flight data exchange messages
  - System performance degradation under the heavy synchronous data processing
  - Cyber security in the interconnected environment

Risk Analysis & Prevention Suggestion

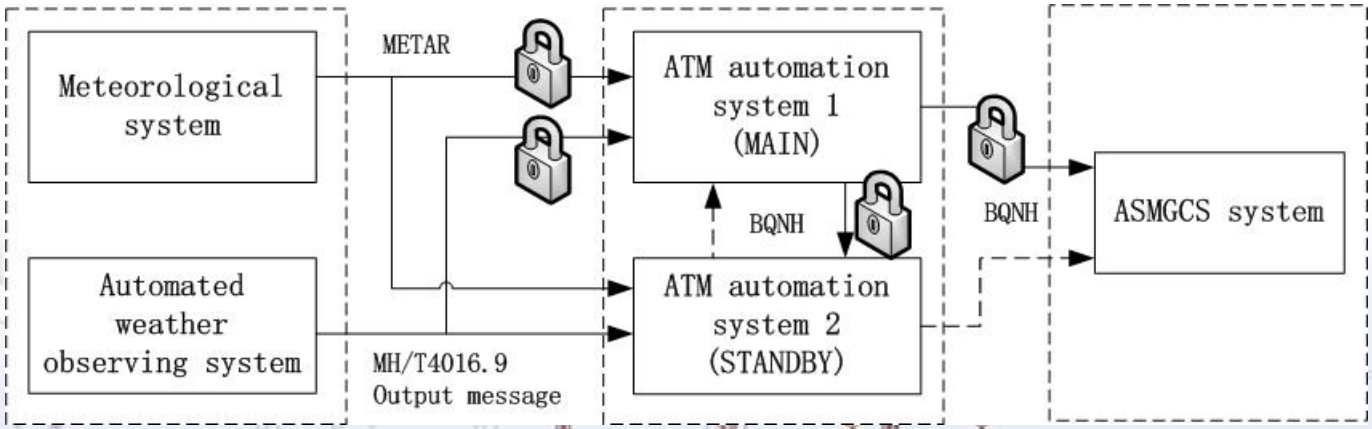
- ***Risk #1 multiple system failures caused by input data or signal***

  METAR ZUCK 221300Z /////MPS 9999 SCT033 ///// Q0000 NOSIG



Risk #1 Risk prevention and control

- Self-protection ability: Data check (drop/manual confirm/Warming)
- Self-healing ability: A reasonable design of system interconnection



Risk Analysis & Prevention Suggestion

- ***Risk #2 Flight plan processing failure caused by the flight data exchange messages***

Although the standby ATC automation system and the A-SMGCS are updated by the operational data from the main ATC automation system, the three systems manage the flight plan life cycle respectively, and they are still receiving AFTN messages by them own. It is a big challenge to balance the benefits of unified processing outcomes and independent maintenance of flight plans among different interconnected systems

Risk Analysis & Prevention Suggestion

- ***Risk #3 System performance degradation under the heavy synchronous data processing***

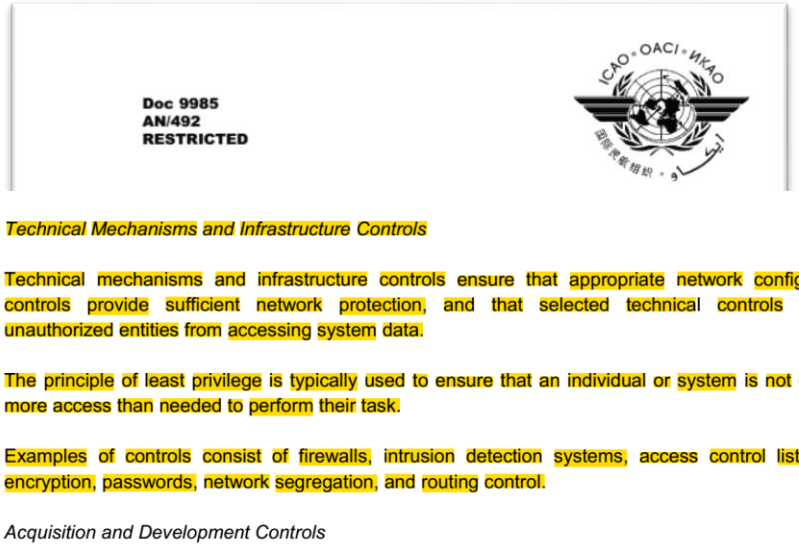
Chongqing ATC center in where the daily flight number is about ***1200***, every day the main automation system sends ***45,000,000 to 50,000,000*** Cat I/B data packets to standby system for synchronization

Risk Analysis & Prevention Suggestion

- ***Risk #3 System performance degradation under the heavy synchronous data processing***
  - ***Data filtering*** can be effectively reduced load of the system
  - ***Flow control*** at the software interface level to limit the amount of data transferred from the interface to the core processing module

☐ *Risk #4 Cyber security in the interconnected environment*

- Reliability, efficiency and security of TCP/IP network
- The notice in the ICAO Doc9985
- Expanding and blurred boundary of the network



Doc 9985
AN/492
RESTRICTED

6) *Technical Mechanisms and Infrastructure Controls*

Technical mechanisms and infrastructure controls ensure that appropriate network configuration controls provide sufficient network protection, and that selected technical controls prevent unauthorized entities from accessing system data.

The principle of least privilege is typically used to ensure that an individual or system is not granted more access than needed to perform their task.

Examples of controls consist of firewalls, intrusion detection systems, access control lists, data encryption, passwords, network segregation, and routing control.

7) *Acquisition and Development Controls*

Risk Analysis & Prevention Suggestion

☐ *Risk #4 Cyber security in the interconnected environment*

A firewall (FW) or an intrusion prevention system (IPS) requires need to be add into automation system. At the same time, in the network configuration with external interconnection, based on static/dynamic Layer 3 routing control (IP route), combined with address translation (NAT), access control list (ACL), hot backup routing protocol (HSRP) multiple strategies The overall network solution needs to be researched and proposed to enhance the robustness of the automation system interconnection network.

Risk Analysis & Prevention Suggestion

- ***Use the standby automation system to prevent* unpredictable *risk***

  - difficulties in the trouble-shooting
  - Use the standby system

Conclusion & Proposal

- To meet the requirements for “coordination” and “intelligence” in air traffic control work, the ATM automation system has developed from a closed, independent, simple system to the system which is open, coordinated, and complex. Leading the system interactions and data sharing will be the new mission for automation systems in the future. While enjoying the efficiency brought by the system interconnection, identifying and reducing the operational risks and potential threats of the automation system in the connected environment will be the next important research topic.

ICAO

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