International Civil Aviation Organization

The First Meeting of Air Traffic Management Automation System Task Force of APANPIRG (ATMASTF/1)

Web-conference, 28 – 30October2020

Agenda Item 5: Issues and Challenges in implementation

5.9 Cyber threats and mitigation measures

CYBERSECURITYCONTROL FOR ATM AUTOMATION SYSTEM IN THE INTERCONNECTION ENVIRONMENT

(Presented by China)

SUMMARY

This paper presents the requirements of the cybersecurity control for the ATM automation system based on ICAO documentation and provides measures and suggestions in a further step.

1. INTRODUCTION

1.1 In recent years, with the implementation of data exchange between ATM automation system and other external systems, the ATM automation system is no longer a closed and individual system which only depends on radar signal and AFTN message through serial port connection for safety purpose. It has developed to work in the interconnection environment based on IP network. The system network has been expanded from the local area network (LAN) in a single ATC center to the wide area network (WAN) where there are many external partners expecting to align with ATM automation system, such as airports, airlines, and even another ATC centers in different region and country. With the expansion and extension of network dimensions, the ATM automation system will meet more and more potential cyber threats and risks in the future.

1.2 To address the growing concerns on cyber security, ICAO published Doc 9985 -*ATM Security Manual* in 2013 setting out the guidelines for ANSPs to protect critical cyber ICT systems. It is clearly notified in Doc 9985 that the ATSP should be content with cyber security measures according to the NCASP and national programs. In 2019, the Standardization Administration of People's Republic of China (SAC) published the latest version *GB/T 22239-2019 Information security technology- Baseline for classified protection of cyber security,* in which it defined five security levels for the national information systems according to the importance and the harmfulness after being damaged. The ATM automation system is required to meet the baseline of level-3.

2. DISCUSSION

2.1 It is recommended in the ICAO Doc 9985 that cybersecurity controls of ICT systems can be organized into nine categories:

1 ） Organizational direction and policy controls
2 ） Organization, culture, and management controls
3 ） Human resources controls
4 ） Physical and environmental security controls
5 ） Operation of ICT system controls
6 ） Technical mechanisms and infrastructure controls
7 ） Acquisition and development controls
8 ） Monitoring and audit controls
9 ） Compliance controls

2.2 According to the Chinese GB/T 22239-2019 standard, the level-3 ICT systems is required to ensure security from the following components:

1 ） Physical environment security
2 ） Communication network and system boundary security
3 ） Computing environment security
4 ） Security management and audit center
5 ） Management policy, organization, workers
6 ） Management of the construction, operation and maintenance.

2.3 Based on the guidelines of ICAO Doc 9985, and taking the Chinese national classified protection requirements for reference, a simplified cyber security control model for ATM automation system is summarized with the four components.

1 ） Operation environment
2 ） Technical mechanisms
3 ） Human resources
4 ） Management

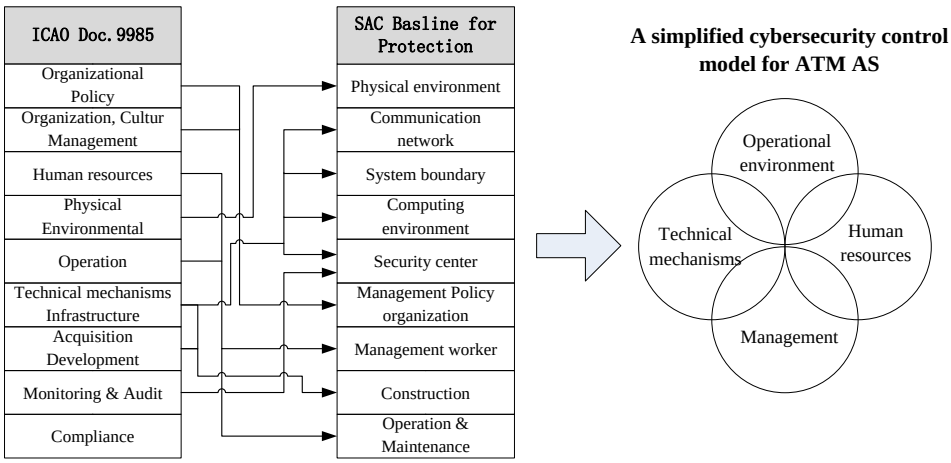

Fig.1 Simplified cyber security model for ATM AS

2.4 In the four components described above, it is supposed to pay special attention on the technical mechanisms. The PDRR security model is widely used in the construction of technical mechanism aspect of the cyber security control. It consists of four modules: Protection, Detection,

Response, and Recovery. Protection is the most important part in the PDRR model to defence against cyber-attacks on the first line. A powerful protection can prevent the occurrence of attacks in advance and reduce most intrusions. Detection is the next key modules. The system detects cyber-attacks that have been failed to be prevented and reacts to it and recovers in the first place.

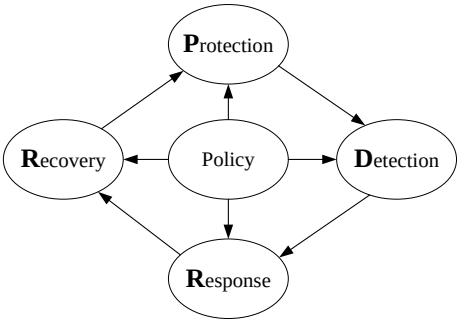

Fig.2 The PDRR security model

2.5 Considering the operation of ATM automation system, it is recommended to give priority to P(protection) and D(detection)to set up technical mechanisms control for ATM automation system. As shown in the fig.3, it is suggested to optimize system network structure, deploy security equipment and related configuration strategies at the boundary, and improve the system capability to prevent and detect external threats. The following measures should be concerned:

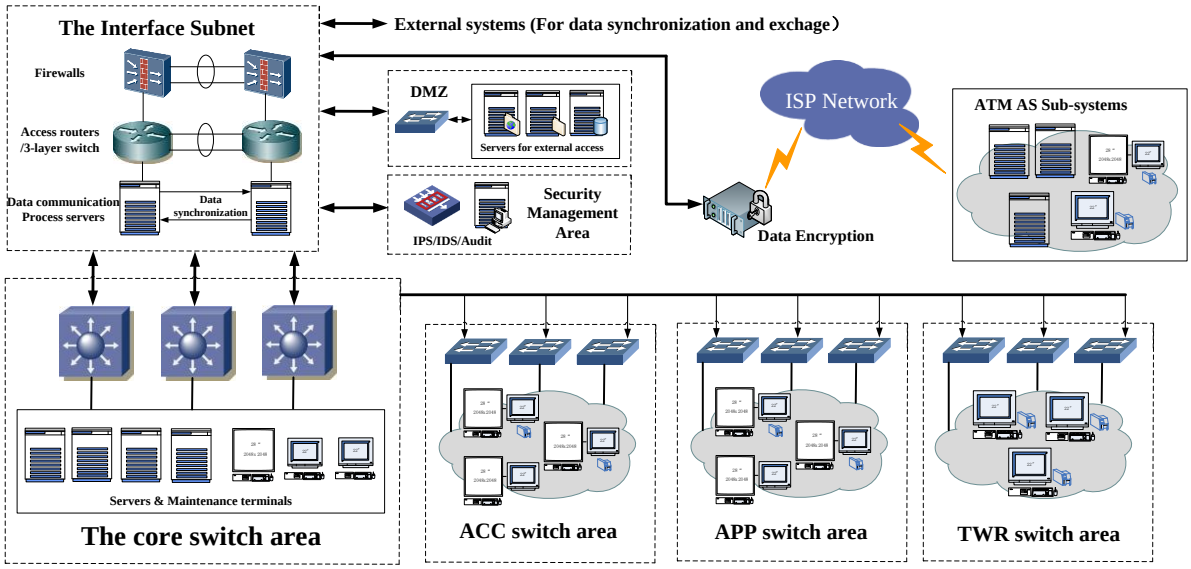

Fig.3 The network structure optimization of ATM AS for cybersecurity

2.5.1 Building interface subnet at the boundary of ATM automation system linked with external systems through the IP routing is a considerably wise and strong approach. On the other hand, deploying network security devices around the interface subnet and configuring security policies such as access control list (ACL), address translation (NAT), black and white list have a great effect on the protection ability of interface subnet.

2.5.2 In addition to the real-time communications and structural data exchanges, the ATM automation system sends or receives certain kinds of text messages or file-format information with external systems. It requires ATM automation system to provide a node for external access. By the means of establishing demilitarized zone (DMZ)to input and output that low real-time data, it can effectively isolate the operational ATM automation system from direct access to external systems through internal nodes.

2.5.3 Different from the Internet communication, under normal circumstances, the legal and useful data interconnections to ATM automation system are previously defined and known. It is supposed to deploy the intrusion detection system （IDS）or intrusion prevention system （IPS） to detect the unauthorized and illegal links. According to different types of data interaction, priority can be categorized with responding rules so that security control strategy can be implemented in different levels of data interconnection.

2.5.4 With the optimization and adjustment of airspace structure, the ACC-TMA-TWR operational mode will be widely used in Chinese seven regional ATC centers. The second ATC center and the second airport for each region are in plan and under consideration in order to keep pace with the rapid growth of flight flow. The ATM automation system with remote structure composed of multiple subsystems will be more and more extensively applied. In the long-distance transmission between the subsystems of internet service provider (ISP), data encryption protection including physical encryption, IP sec and other technologies needs to be used to prevent the occurrence of data risks from the network side of the ISP, and ensure that the interactive data between the subsystems is complete and hardly tampered or stolen.

2.5.5 The increase of flight flow and refining of ATC sectors leads to the aggrandizement of ATM automation system scale. There is a large number of nodes participating in data transmission and exchange in the system local network. Dividing the network into multiple virtual local areas is the frequently used method, by which not only helps to improve the stability and security of the local network of system, but also controls the communication range of each node, in order to lay the foundation for the deployment of advanced strategies such as security audit and network behavior management in the further step.

2.6 Suggestion for the follow-up actions

2.6.1 To research and develop an overall technical solution for cyber security for ATM automation system. To verify the feasibility, effectiveness and applicability of the solution by ATM automation test and verity system (TVS).

2.6.2 To apply the solution to small or medium-sized ATM automation system to verify the effectiveness and stability of the solution in practical operation.

2.6.3 To form a consensus on the cybersecurity of ATM automation system. To unify the design concept, and gradually establish the correspondingly technical industry standards, in order to provide guidelines for the future ATM automation system design.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) encourage states to carry out specific researches and actions further more to improve the cybersecurity control, especially the technical mechanisms control for ATM automation system.

– – – – – – – – – – – – – –