The CNMS Network Information Security Research Based on Risk Assessment

Jiang Jingyi, Zhongming, He guosheng, Wang qingqi

Middle South Regional ATMB CAAC(New Baiyun International Airport air traffic controlling Building Flight Service Center Room 318), Guangzhou 510000,China
290121643@qq.com

Abstract. With the deepening of the information level of civil aviation information, CNMS system network information security problems highlight. There are basically no corresponding domestic and international network security research methods. This paper presents a method of CNMS network information security research based on risk assessment. Based on the analysis of network architecture, the CNMS network security risk assessment is carried out. Based on the evaluation result and the advanced technology, the security improvement scheme from the main to the secondary is proposed. Finally, an example shows that this method can effectively analyze and solve the CNMS network information security problems.

1. Introduction
The development of large data is on the civil aviation industry have a profound impact, the construction of civil aviation air traffic control data center is the trend. Therefore, to strengthen the protection of civil aviation air traffic control system of network information security rose to an important strategic position. At present, Civil Notam management system (CNMS system) as a three-level system, with a large number of internal sensitive data, was included in the list of national important information systems. CNMS system is relying on civil aviation ATM data communication network interconnection of the air traffic control system with the enterprise network (Intranet network), and strict physically isolates with the Internet. Operating systems, databases and other common software localization rate is very low. Only relying on physical isolation needs to be improved and the strict physically isolation makes the lack of external data exchange means. Therefore, CNMS system network information security issues need to be improved. However, there is basically no method for civil aviation CNMS system, and its network security problem has not been effectively solved.

This paper presents a research on CNMS network information security based on risk assessment. First, the topology of CNMS is analyzed. Secondly, complete the CNMS network information security risk assessment. Finally, on the basis of risk assessment, propose the corresponding CNMS network information security improvement scheme by use of the current advanced network information security technology and method. This method can analyze the problem of network information security in CNMS system more effectively and classify the risk, so as to provide an effective solution which can better targeted to the problem by integrating advanced technology.

2. Analysis of CNMS Network Architecture
Internet, the network are basically using C/S architecture model, usually including the main server, client, network connectivity devices. This paper analyzes the CNMS basic network architecture shown in Fig. 1 as an example. The CNMS system consists of the CNMS server 1 and the CNMS server 2, and the CNMS spare server constituting the standby system. The main system and the standby system belong to two network segments, which are connected through the optical fiber and the switch.

![CNMS basic network architecture topology](image)

Figure 1 CNMS basic network architecture topology

3. Risk assessments

3.1. Asset identification

By analyzing the business process and function of the CNMS system, it is necessary to identify the CIA information data and the surrounding environment from the security requirements of the integrity, usability and confidentiality of the information data [2]. The list of specific assets is shown in "Asset ID" and "Asset Name" in Table 1 below. Assets the asset value of all assets by the multiplication method. The calculation formula (1-1) is as follows:

\[
V = f(x, y, z) = \sqrt[3]{x \times y \times z}
\]

Where V is the asset value, x is the confidentiality, y is the integrity, and z is the usability. In this formula, the asset value of the assets of the system is obtained as shown in Table 3 to Table 6, "Asset Value". In order to correspond to security attributes, the asset is divided into five levels according to the final assignment. The higher the asset grade value indicates the more important the asset is.
### Table 1 List of assets

| Asset ID | Asset name                  | Confidentiality | Integrity | Availability | Asset value | Asset grade value |
|----------|-----------------------------|-----------------|-----------|--------------|-------------|-------------------|
| A01      | cnms server 1               | y               | y         | y            | 5           | 5                 |
| A02      | cnms server 2               | y               | y         | y            | 5           | 5                 |
| A03      | disk array                 | 3               | y         | y            | 4.4         | 5                 |
| A04      | SAN switch                 | 4               | y         | y            | 4.5         | 5                 |
| A05      | main switch                | 3               | y         | y            | 4.2         | 4                 |
| A06      | alternate switch           | 3               | y         | y            | 3.7         | 4                 |
| A07      | NOF Switch                  | 3               | y         | y            | 4.2         | 4                 |
| A08      | CNMS Standby Server switch (old network segment) | 5 | 5 | 5 | 5 | 5 |
| A09      | motor room switch           | 3               | y         | y            | 3.7         | 4                 |
| A10      | NOF Terminal 1#             | 2               | 2         | 2            | 2           | 2                 |
| A11      | NOF Terminal 2#             | 2               | 2         | 2            | 2           | 2                 |
| A12      | telegraph interface terminal | 3               | 5         | 5            | 4.4         | 5                 |
| A13      | network security regime     | 1               | 4         | 4            | 2.8         | 3                 |
| A14      | staff file                  | 5               | 5         | 2            | 3.2         | 3                 |
| A15      | backup data                 | 5               | 5         | 3            | 3.9         | 4                 |
| A16      | emergency, backup system    | 1               | 4         | 4            | 2.8         | 3                 |
| A17      | ordinary users              | 5               | 2         | 2            | 2.5         | 2                 |

### 3.2. Threat identification

A security threat is a potential factor that constitutes damage to the system and its assets. According to the frequency of the threat, it is divided into from 1 to 5, respectively from low to high 5 different levels. By using the questionnaire and technical testing to obtain the threat of information, the questionnaire mainly collects some management-related threats, and the technical testing mainly obtains the threat of the system by analyzing the IDS log information. Table 2 shows the types of threats and the frequency of the threat.

### Table 2 Types of security threats faced by information systems

| Threat ID | Threat Class                          | Frequency |
|-----------|---------------------------------------|-----------|
| T01       | hardware failure                      | 2         |
| T02       | software failure                      | 2         |
| T03       | malicious code and virus              | 4         |
| T04       | Physical Environmental Threats        | 1         |
| T05       | Unauthorized access                   | 4         |
| T06       | Permission Abuse                      | 3         |
| T07       | detection steal                       | 3         |
| T08       | data tampering                        | 3         |
| T09       | Vulnerability utilization             | 3         |
| T10       | physical attack                       | 1         |
3.3. vulnerability identification
The vulnerability assessment of this CNMS system is based on strategic document analysis, network architecture analysis, business process analysis, tool scanning, configuration verification and so on, and combining the detection results of the national network information security hierarchy protection. According to the severity of the vulnerability, it is divided into from 1 to 5, respectively, from low to high 5 different grades.

Table 3 Vulnerability identification results

| Vulnerability ID | Vulnerability Name                          | Asset ID | Severity |
|------------------|--------------------------------------------|----------|----------|
| V01              | database vulnerabilities                   | A08      | 5        |
| V02              | Firewall mission                           | A09      | 5        |
| V03              | IPS mission                                | A02      | 5        |
| V04              | anti-virus software mission                | A10      | 5        |
| V05              | anti-theft measures mission                | A01      | 4        |
| V06              | clear text transmission                    | A05      | 3        |
| V07              | database authorization too large           | A01      | 2        |
| V08              | Database Password Configuration            | A02      | 2        |

3.4. Risk analysis
A risk assessment algorithm uses the risk-related factor relation model and the comprehensive evaluation method combining qualitative and quantitative. In the completion of asset identification, threat identification, vulnerability identification, it use the function of the calculation method to determine the possibility of an unsafe event and the impact of the loss which the threat use vulnerability in the value of assets led to, that is security risks. Use the following function paradigm to express [3]:

\[ R(A,V,T) = R(L(V,T),F(Ia,Va)) \]

R represents a security risk calculation function. A represents an asset, the value of the asset acting on a security event. T represents a threat. V represents vulnerability, the severity of the vulnerability. L means a possibility of an unsafe event which the threat use vulnerability in the value of assets led to; F means the loss of the security incident. L function, F function and R function are calculated by the combination of two-dimensional matrix method and probability level judgment criterion. Details see reference [5] content. This CNMS system evaluates the system asset risk based on the results of asset identification, threat identification and vulnerability identification. The results are obtained in table 4 on the basic data of table 2 and 3.

Table 4 Asset risk analysis results

| A ID | T ID | V ID | F Grade | L Grade | Risk Value | Risk Level |
|------|------|------|---------|---------|------------|------------|
| A01  | T07  | V05  | 4       | 5       | 23         | high       |
|      | T06  | V07  | 2       | 3       | 9          | Low        |
|      | T05  | V08  | 3       | 3       | 13         | Middle     |
|      | T03  | V03  | 5       | 5       | 25         | Very high  |
| A08  | T08  | V09  | 2       | 3       | 9          | Low        |
|      | T09  | V01  | 4       | 5       | 23         | high       |
| A10  | T03  | V10  | 3       | 2       | 11         | Low        |
|      | T05  | V04  | 5       | 4       | 23         | high       |
4. CNMS network information security solution

According to the results of CNMS network security risk assessment, the following security solutions \cite{4,5} are proposed in consideration of the overall security requirements of CNMS. Give priority to the risk of high risk, taking into account of dealing with low risk.

1) The use of three regional network security structures. Between the external network and within the network to add a subnet by the security proxy server and dual firewall, play a buffer isolation role. The proxy server can only send read data to the network requirements, there is no permission to write data. In this way, both CNMS system and external network connected to achieve the purpose of data sharing; but also relatively isolated to protect the security of intranet data security.

(2) Increase the eight black shield firewall system the integration of hardware and software design, after curing and transformation of the safe operating system use, greatly enhance the overall security of the firewall.

(3) Increase the black shield intrusion detection system (HDIDS) to achieve real-time security monitoring, with the black shield firewall system work together, 24 hours of uninterrupted data packet on the protected network segment to listen and analysis, real-time monitoring of intrusion, Real-time record of attack events, and can block the attack behavior based on the attack response to the pre-set.

(4) Increase Rising online version anti-virus software, unified control by the central console management, remote installation, distribution killing, to achieve a unified network anti-virus. This technology can ensure that anti-virus operation will not hurt the operating system kernel, while ensuring that kill the virus.

(5) In the CNMS listener, add IP limit settings, allowing only the specified IP can enter the Oracle database, other IP cannot login, so you can solve Oracle's long-range Core RDBMS vulnerability.

(6) Propose remote management of the database using eavesdropping measures, such as SSL. Network equipment using SSH or https for remote connection, the database should be set to verify the transmission process password connection encryption.

In addition, for the other medium and low risk of CNMS, we can further strengthen the network security management measures, such as increasing the password responsibility, using more than two combination authentication technology, increasing the integrity inspection tools to check the integrity of important documents. Using the same method to conduct a risk assessment of the CNMS system again, we can get the risk statistics table of the CNMS system before and after the transformation, as shown in Table 5:

| Asset risk level statistics table |
|----------------------------------|
| **risk** | Very high | high | middle | low | Very low |
| Before transformation | 2 | 3 | 2 | 4 | 1 |
| After transformation | 0 | 0 | 2 | 3 | 3 |

The method proposed in this paper can combine security policy, hardware and software to form a unified defense system, realize data sharing to a certain extent and effectively reduce the network security risk.

5. Conclusions

A practical example shows that the CNMS network information security research based on risk is a kind of targeted and effective research method, which has the following advantages:

1. The combination of qualitative and quantitative methods, the CNMS network information security risk assessment can scientifically and objectively analysis the practical existence of network
problems.

2. this risk assessment method not only to identify the risk, and gives the corresponding risk level value, will propose the final classifiable security improvement program from main to subordinate.

3. the use of the most advanced network security technology and network security products, more effective response to the latest network information security issues.

4. filled with the blank of CNMS network information security research methods, breaking the previous deadlock of only physical isolation method. Not only guarantee the safety of CNMS network information, but also enable the information to have massive data to achieve sharing, improve the utilization of information.

References:
[1] Computer network information security and protection [J]. Wan Hui-yong, Xiong Xiaojun. Network Security Technology and Application .2016 (03)
[2] Network system security situation assessment research [J]. Chen Xiuzhen, Zheng Qinghua, Guan Xiaohong, Lin Chengguang. Journal of Xi'an Jiaotong University .2004 (04)
[3] Computer network information security risk assessment criteria and methods [D]. Zhang Wei. Tianjin. Tianjin University School of Electronic Engineering Information .2009
[4] Application of active defense technology in communication network security project [J]. Dong Xiquan, Lin Li, Zhang Xiaojun, Ren Peng. Information Security and Technology .2016 (01)
[5] Alberts, Christopher J. and Dorofee, Audery J.OCTAVE Method Implementation Guide v2.0. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001