Research and Application of the Network Security Monitoring Capability Evaluation Model of Power Control System Based on AHP and Fuzzy Comprehensive Evaluation

Penghao Wang\textsuperscript{1*}, Shaobo Wang\textsuperscript{1}, Lijun Chi\textsuperscript{1}, Xiaokai Ren\textsuperscript{2}, Wei Wu\textsuperscript{1} and Wenjie Cheng\textsuperscript{1}

\textsuperscript{1} State Grid Shijiazhuang Power Supply Company of Hebei Electric Power Co., Ltd, Shijiazhuang, Hebei, 050000, China
\textsuperscript{2} State Grid Hebei Electric Power Co., Ltd, Shijiazhuang, Hebei, 050000, China
*Corresponding author’s e-mail: wangpenghao23@foxmail.com

Abstract. In recent years, China’s cyberspace security is facing increasingly severe challenges. As the national key basic information infrastructure, power control system is very important which is related to the national economy and the people’s livelihood. So network security of power control system should be taken seriously. The network security monitoring capability of power control system has a direct impact on the security of power business such as power production and supply. However, there are few studies on the evaluation of its network security monitoring capability. This paper puts forward the network security monitoring capability evaluation model of power control system based on AHP and fuzzy comprehensive evaluation, according to the research of public network security management capability evaluation, the particularity of network security monitoring system of power control system and the investigation opinions of 20 expert teams in power industry’s network security field. Then, the model is used to evaluate the network security monitoring capability of three municipal power control systems, and the final scores are 93.09, 88.65 and 90.17 respectively. The model established in this paper realizes the quantitative evaluation of the network security monitoring capability of the power control system. And it will help the power company to carry out targeted rectification and improvement according to the calculating result of this model. So the research and application in this paper has a certain practical engineering significance.

1. Introduction
With the rapid development of China’s power industry, the business scope of power system is expanding and the new technologies are widely used. The power dispatching data network is gradually integrated in all links of power generation, transmission, transformation, distribution and power consumption, and it has become a key component of power system\textsuperscript{[1-2]}. However, the current network security situation at home and abroad is grim. Organized network attacks such as the infection of Stuxnet in Iran’s nuclear power plant and the infection of blackmail virus in the largest natural gas and diesel transportation pipeline company in the United States occur frequently. In particular, attacks against power, oil and other energy industries are increasing year by year\textsuperscript{[3]}. As the first batch of national key basic information infrastructure, the network security of power control system has attracted more and more attention. With the massive access of photovoltaic, wind power and other new energy stations in recent years, the network space of power dispatching data network has expanded rapidly. Now, the network
security of power control system is facing unprecedented pressure with the rapid change of network attack means. However, there are few studies and applications on the evaluation of network security monitoring capability of power control system. Therefore, the research on this topic has certain engineering significance and can provide quantitative basis for the evaluation of network security monitoring capability of power control system. So, this paper studies the evaluation of network security monitoring capability of power control system comprehensively considering the AHP and fuzzy comprehensive evaluation widely used in the evaluation of public network security management ability and the power control system is different from public network security, has the characteristics of complex structure, wide boundary and special service[4].

2. Evaluation indexes
This section introduces the relevant theories and technologies of the network security monitoring system and network security management platform of the power control system. Then the evaluation index of the network security monitoring capability will be determined according to the expert experience, and the specific meaning of each index will be expounded.

2.1. The network security monitoring system of electric power control system
As a national key information infrastructure, the network security monitoring system of power control system is also relatively complete[5]. At present, according to the design principle of “self perception, distributed collection and unified management”, the network security monitoring system of power control system has built a complete system that can perceive, collect and manage its own network security information.

![Figure 1. The network security monitoring system of electric power control system](image)

- Self perception. The monitoring system relies on the network security monitoring device to monitor and report the network security alarm information of servers, workstations, switches, vertical encryption devices, network security isolation devices and other equipment deployed in the master station of power dispatch system, substations and power plants in real time.
- Distributed acquisition. Relying on the power dispatching data network to transmit, communicate and interact the network security data of all master stations, power plants, substations, power distribution systems and load control systems.
- Unified management. Relying on the network security management platform, all data in the network security monitoring system can be summarized, analyzed and calculated, and the functions of real-time monitoring, alarm, analysis, audit and verification can be realized. At the same time, the network security management platforms deployed in national, provincial and
municipal master stations can be cascaded and accessed to each other, so as to realize the full coverage of network security monitoring of power control system.

2.2. The evaluation indexes of network security monitoring capability

Compared with the public network security monitoring system, the network security monitoring system of power control system has the characteristics of large system, large amount of equipment, high reliability and real-time performance in data transmission. Therefore, it is necessary to design a series of evaluation indexes that can reflect the network security monitoring capability of power control system more accurately. Considering the requirements for network security of power control system in various laws and standards[6], and the investigation opinions of 20 experts in power industry’s network security field, this paper finally proposes 3 aspects and 12 indexes for the evaluation of network security monitoring capability of power control system, as shown in table 1.

| Table 1. The evaluation indexes of network security monitoring capability |
| Aspects               | Indexes                                                                 |
|-----------------------|-------------------------------------------------------------------------|
| The integrity of system | The safety protection hardware                                              |
|                       | The safety protection software                                           |
|                       | The external physical protection                                         |
|                       | The emergency safeguards                                                 |
|                       | The encryption rate of data communication                                 |
| The compliance rate of index | The reliability of network security management platform                         |
|                       | The reliability of safety protection equipment                            |
|                       | The timeliness rate of alarm response                                    |
|                       | The management system of network security                                 |
|                       | Implement safety protection measures totally                             |
|                       | Organize emergency drill regularly                                       |
|                       | The network security ability of staff                                     |

2.3. The meaning of evaluation indexes

The evaluation of network security monitoring capability of power control system mainly involves three aspects: the integrity of system, the compliance rate of index and the effectiveness of management. Each aspect has four evaluation indexes, and the specific meanings of the indexes are as follows:

- The safety protection hardware. It refers to whether the network security protection hardware such as network security isolation device, vertical encryption authentication device and network security monitoring device deployed by the monitoring system are complete.
- The safety protection software. It refers to whether the network security protection software such as anti-virus software, malicious code monitoring system, intrusion detection system and other network security protection software deployed by the monitoring system are complete.
- The external physical protection. It refers to whether the access control system and security measures of important places such as monitoring hall and equipment room meet the requirements.
- The emergency safeguards. It refers to whether the emergency safeguards such as disaster recovery, data recovery and major risk safeguards are complete.
- The encryption rate of data communication. It refers to the encryption rate of data transmission between the master stations and power plant and substation.
- The reliability of network security management platform. It refers to whether the server and workstation of the network security management platform operate reliably, and whether the cascade and access communication of the upper and lower platforms are reliable.
- The reliability of safety protection equipment. It refers to whether the security equipment connected to the network security management platform is online and working normally.
• The timeliness rate of alarm response. It refers to the compliance rate that when the network security management platform monitors the security alarm, the attendant can handle it in time.
• The management system of network security. It refers to whether the security equipment management, personnel on duty management, operation monitoring management and other management systems of the monitoring system are complete.
• Implement safety protection measures totally. It refers to whether the network security protection requirements such as network security vulnerability rectification, security equipment upgrading and special security inspection required by the superior are totally implemented.
• Organize emergency drill regularly. It refers to whether emergency drills for network security of power control system are organized regularly.
• The network security ability of staff. It refers to the network security ability of staff engaged in network security monitoring, such as malicious virus blocking and emergency disposal.

3. Evaluation model
According to the evaluation indexes of network security monitoring capability proposed above, this paper establishes the evaluation model of network security monitoring capability by using AHP and fuzzy comprehensive evaluation. The model combines the advantages of AHP and fuzzy comprehensive evaluation[7-8], and it can comprehensively calculate the evaluation score of monitoring capability according to the opinions of expert team, so as to realize the comprehensive evaluation of network security monitoring capability of power control system.

3.1. The hierarchy structure
As the evaluation indexes of network security monitoring capability have been proposed above, the hierarchy structure can be established according to AHP. In the hierarchy structure, the network security monitoring capability is taken as the target layer, The integrity of system, the compliance rate of index and the effectiveness of management are taken as the criterion layer, and 12 indexes such as security protection hardware and security protection software are taken as the index layer, as shown in figure 2.

![Figure 2. The hierarchy structure of network security monitoring capability](image)

3.2. Calculation of index weight
The hierarchy structure defines the subordinate relationship among target layer, criterion layer and index layer. Now it is necessary to calculate the weight matrix of the criterion layer according to the contribution of criterion layer elements to target layer and calculate the weight matrix of the index layer according to the contribution of index layer elements to criterion layer.
3.2.1. The pairwise comparison matrix.

Experts evaluate the importance of each element of the criterion layer and the index layer according to their own work experience and professional knowledge. According to the scoring results of experts, the pairwise comparison matrix \( A \) that can reflect the degree of interaction between two elements can be calculated based on the Saaty scale[9].

\[
A = (a_{ij})_{n \times n} \\
a_{ij} = 1/a_{ji}
\]  

In the above formula (1), \( a_{ij} \) represents the scale value of the element.

3.2.2. Normalization of pairwise comparison matrix.

The pairwise comparison matrix \( A \) is normalized to the transition matrix \( B \). And the element \( b_{ij} \) in the transition matrix \( B \) is calculated by the following formula:

\[
b_{ij} = \frac{a_{ij}}{\sum_{l=1}^{n} a_{lj}}
\]  

In the above formula (2), \( \sum_{l=1}^{n} a_{lj} \) represents the sum of each column in matrix \( A \).

3.2.3. Calculation of weight matrix

The weight matrix \( W \) can be obtained by normalizing the eigenvector of matrix \( B \), and the element of the weight matrix \( w_i \) is calculated by the following formula:

\[
w_{ij} = \frac{\sum_{j=1}^{m} b_{ij}}{m}
\]  

3.2.4. Consistency test

In order to test the effectiveness of expert evaluation results and eliminate the differences caused by subjective opinions, it is necessary to test the consistency of calculation results. First, the value of the weight matrix \( W \)’s maximum eigenvalue \( \lambda_{\text{max}} \) can be calculated using the formula (4). And the consistency index C.I. and consistency ratio C.R. are also calculated with \( \lambda_{\text{max}} \) by formula (5) and (6).

\[
\lambda_{\text{max}} = \sum_{l=1}^{n} \frac{AW}{nW}
\]  

\[
\text{C.I.} = \frac{\lambda_{\text{max}} - n}{n-1}
\]  

\[
\text{C.R.} = \frac{\text{C.I.}}{R.I.}
\]  

In the above formula (6), R.I. takes different values with the order of the matrix[10]. If the consistency ratio C.R. is less than 0.1, it indicates that the calculation result is acceptable, otherwise it indicates that the result is unacceptable.

3.3. Fuzzy comprehensive evaluation

Since many evaluation indexes of network security monitoring capability of power control system cannot be obtained by quantification, this paper adopts fuzzy comprehensive evaluation method to realize the quantitative evaluation of network security monitoring capability by establishing factor set, weight set and comment set.

3.3.1. Factor set, weight set and comment set

The factor set can be established according to the hierarchy structure determined in section 3.1, and the weight set can be established according to the weight matrix in section 3.2. The monitoring capability is divided into five levels. The comment set \( V = \{\text{excellent, good, medium, poor, very poor}\} \). The score vector is set as \( V^T = \{95, 85, 75, 65, 50\}^T \).
3.3.2. Fuzzy evaluation matrix
According to the evaluation results of the expert team on the factors of index layer, an evaluation matrix will be established. After normalizing the evaluation matrix, the first-order fuzzy evaluation matrix $R$ is obtained.

$$R = (r_{ij})_{n \times m}$$

In the above formula (7), $r_{ij}$ represents the normalized evaluation results of the index layer elements.

3.3.3. Results of fuzzy evaluation
From the first-order fuzzy matrix $R$ and the index layer weight matrix $W_i$, the first-order fuzzy evaluation result $C_i$ can be calculated. Then, according to the three first-order fuzzy evaluation results $C_1$, $C_2$, $C_3$ and the criterion layer weight matrix $W_p$, the second-order fuzzy evaluation result $D$ can be calculated.

$$C_i = W_i R_i$$
$$D = W_p \begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix}$$

3.3.4. Calculating the final score
The final score of the network security monitoring capability $S$ can be calculated by using the second-order fuzzy evaluation result $D$ and the score vector $V^T$.

$$S = D V^T$$

4. Application of the model
In this paper, an expert team composed of 20 network security experts of power control system is established, and the expert team are invited to determine the weight matrix of criterion layer and index layer by anonymous scoring and evaluation. At the same time, three municipal power control systems are selected, and the expert team are invited to evaluate the network security monitoring capability of these three systems respectively. The calculation results are as follows.

4.1. Calculation of index weight
According to the evaluation model established above, the expert team evaluate the importance of criteria layer elements and index layer elements. Taking the evaluation results of the criterion layer as example, the paired comparison matrix $A_1$ calculated by using the expert scoring results which are shown in table 2.

| $A_1$ | The integrity of system | The compliance rate of index | The effectiveness of management |
|-------|-------------------------|-----------------------------|-------------------------------|
| The integrity of system | 1 | 2 | 3 |
| The compliance rate of index | 1/2 | 1 | 2 |
| The effectiveness of management | 1/3 | 1/2 | 1 |

The criterion layer’s normalized transition matrix $B_1$ and weight matrix $W_p$ can be calculated by using formula (2) and (3). The results are shown in table 3:
Table 3. The criterion layer’s normalized transition matrix $B_1$ and weight matrix $W_p$

| $B_1$               | The integrity of system | The compliance rate of index | The effectiveness of management |
|---------------------|-------------------------|------------------------------|--------------------------------|
| The integrity of system | 0.545                   | 0.571                        | 0.500                          |
| The compliance rate of index | 0.273                   | 0.286                        | 0.333                          |
| The effectiveness of management | 0.182                   | 0.143                        | 0.167                          |
| $W_p$               | 0.539                   | 0.297                        | 0.164                          |

$\lambda_{\text{max}}$ is calculated as 3.0097 according to formula (4). Since it is a third-order matrix, R.I. is taken as 0.58, and C.R. is calculated as 0.0079 according to formula (5) and formula (6). Through the consistency test, C.R. is less than 0.1, so the calculation results are acceptable.

Similarly, using the calculation process above, the weight matrix of each index layer can be calculated according to the evaluation results of the expert team, as shown in table 4.

Table 4. Every index layer’s weight matrix $W_1$, $W_2$, and $W_3$

| Index layer 1 | The safety protection hardware software | The safety protection | The external physical protection | The emergency safeguards |
|---------------|-----------------------------------------|-----------------------|---------------------------------|--------------------------|
| $W_1$         | 0.475                                   | 0.338                 | 0.115                           | 0.073                    |
| Index layer 2 | The encryption rate of data communication | The reliability of network security management platform | The reliability of safety protection equipment | The timeliness rate of alarm response |
| $W_2$         | 0.265                                   | 0.409                 | 0.215                           | 0.110                    |
| Index layer 3 | The management system of network security | Organize emergency drill regularly | Implement safety protection measures totally | The network security ability of staff |
| $W_3$         | 0.392                                   | 0.055                 | 0.230                           | 0.324                    |

Through the consistency test, the C.R. are 0.0328, 0.0533 and 0.0622 respectively, which are both less than 0.1, so all calculation results are acceptable.

4.2. Fuzzy comprehensive evaluation

The expert team scores 12 indexes of three municipal power control systems. Taking the calculation process of city A as example, according to the expert team’s evaluation results, the fuzzy evaluation matrix $R_i$ of each index layer can be calculated by formula (7).

The integrity of system’s fuzzy evaluation matrix $R_1$:

$$R_1 = \begin{bmatrix} 0.85 & 0.15 & 0 & 0 & 0 \\ 0.80 & 0.20 & 0 & 0 & 0 \\ 0.95 & 0.05 & 0 & 0 & 0 \\ 0.50 & 0.30 & 0.15 & 0.50 & 0 \end{bmatrix}$$

The compliance rate of index’s fuzzy evaluation matrix $R_2$:

$$R_2 = \begin{bmatrix} 0.95 & 0.05 & 0 & 0 & 0 \\ 1.00 & 0 & 0 & 0 & 0 \\ 0.85 & 0.15 & 0 & 0 & 0 \\ 0.80 & 0.20 & 0 & 0 & 0 \end{bmatrix}$$
The effectiveness of management’s fuzzy evaluation matrix \( R_3 \).
\[
R_3 = \begin{bmatrix}
0.80 & 0.10 & 0.10 & 0 & 0 \\
0.25 & 0.50 & 0.20 & 0.05 & 0 \\
0.85 & 0.15 & 0 & 0 & 0 \\
0.50 & 0.45 & 0.05 & 0 & 0 
\end{bmatrix}
\]

According to the weight matrix \( W_i \) calculated above, the first-order fuzzy evaluation result \( C_i \) is calculated by formula (8).
\[
C_1 = [0.819, 0.166, 0.011, 0.004, 0] \\
C_2 = [0.932, 0.068, 0, 0, 0] \\
C_3 = [0.684, 0.247, 0.066, 0.003, 0]
\]

According to the criterion layer’s weight matrix \( W_p \), the second-order fuzzy evaluation result \( D \) is calculated by formula (9).
\[
D = [0.831, 0.150, 0.017, 0.002, 0]
\]

According to the second-order fuzzy evaluation \( D \) and score vector \( V^T \), the final evaluation score of the city is calculated by formula (10). The score \( S_1 \) is 93.09, indicating that the network security monitoring capability of power control system in city A is excellent.

Similarly, the expert team evaluate the network security monitoring capability of the power control system in city \( B \) and \( C \). And the final score is 88.65 and 90.17, which can objectively reflect the network security monitoring capability of the power control system in city \( B \) and \( C \).

5. Summary

This paper puts forward the network security monitoring capability evaluation model of power control system based on AHP and fuzzy comprehensive evaluation, according to the research of public network security management capability evaluation, the particularity of network security monitoring system of power control system and the investigation opinions of 20 expert teams in power industry’s network security field. In order to verify the effectiveness of the model, the model is used to evaluate the network security monitoring capability of three municipal power control systems. After the expert team’s evaluation and model calculation, the final scores are 93.09, 88.65 and 90.17 respectively, which can objectively reflect its network security monitoring capability.

The model established in this paper realizes the quantitative evaluation of the network security monitoring capability of the power control system. And it will help the power company to carry out targeted rectification and improvement according to the calculating result of this model. So the research and application in this paper has a certain practical engineering significance.

However, there are still some deficiencies in this model. The evaluation indexes and index weights in the model are easily affected by the subjective opinions of the expert team. In the future, scholars can establish a expert team with more quantity and higher level to conduct research, or adopt more advanced theories and methods to study the network security monitoring capability evaluation model of power control system.

Acknowledgments

This work is supported by The Science & Technology Project of State Grid Shijiazhuang Power Supply Company of Hebei Electric Power Co., Ltd.

References

[1] Yao J, Yang S, Gao Z, et al. Development Trend Prospects of Power Dispatching Automation System[J]. Automation of Electric Power Systems, 2007.

[2] Ni Z. Research on Key Technologies of Security Risk Analysis and Prediction of Power Industrial Control Network[D]. Nanjing University of Science and Technology, 2019.

[3] Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon[J]. IEEE Security and Privacy Magazine, 2011, 9(3):49-51.
[4] Xiao Y. Research on the Quality Evaluation System of Network Security Service Project Based on the Case Study of Company C[D]. Beijing University of Posts and Telecommunications. 2020.

[5] Liang N. Research on the Technology of Vulnerability Investigation and Risk Management of Electric Power Monitoring System[J]. Automation Panorama, 2019(S02):5.

[6] Li M A, Zhu G, Lei L U. Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019) Standard Interpretation[J]. Netinfo Security, 2019.

[7] Guo J Y, Zhang Z B, Sun Q Y, et al. Study and Application of Analytic Hierarchy Process[J]. Journal of China Safety Science, 2008, 18(5):6.

[8] Icaga Y. Fuzzy evaluation of water quality classification[J]. Ecological Indicators, 2007, 7(3):710-718.

[9] Deng X, Jia-Ming L I, Zeng H J, et al. Research on Computation Methods of AHP Wight Vector and Its Applications[J]. Mathematics in Practice and Theory, 2012.

[10] Teknomo K. Analytic hierarchy process (AHP) tutorial[J]. Retrieved on January, 2006.