Risk Assessment of Power Monitoring System Based on Fuzzy Analytical Hierarchy Process

Huifeng Li1*, Tiecheng Li1, Qigui Yao3,4, Weixun Li2, Libo Yang2, Guanghui Sun2
1 State Grid Hebei Electric Power Research Institute, Shijiazhuang, Hebei, China
2 State Grid Hebei Electric Power Co.Ltd, Shijiazhuang, Hebei, China
3 Global Energy Interconnection Research Institute Co.Ltd, Nanjing, Jiangsu, China
4 State Grid Key Laboratory of Information & Network Security, Nanjing, Jiangsu, China
*Corresponding author’s e-mail: dyy_lihf@he.sgcc.com.cn

Abstract. The security threat of power monitoring system is increasing, it is valuable to carry out effective risk assessment, which helps to find the security threats of the system in time, then carry out security management and avoid disasters. This paper presents a risk assessment method of power monitoring system based on Fuzzy Analytic Hierarchy Process (FAHP) and CVSS. Firstly, Considering the structure and security requirements of power monitoring system, the analytic hierarchy process (AHP) model is established, and CVSS is used to quantify the evaluation indicators. Then, the fuzzy consistent judgment matrix is constructed by using the results of index quantification by using AHP and fuzzy comprehensive evaluation theory, and the power monitoring system is comprehensively evaluated from the bottom to the top. Finally, the risk evaluation value and safety level of the system are obtained. The example shows that the method can effectively overcome the difficulty of AHP in checking the consistency of judgment matrix, and can effectively quantify the system risk, and provide reference and basis for risk management decision-making of power monitoring system.

1. Introduction
With the development of national informatization, the informatization level of power system is constantly improving, but it also brings more security threats. Power monitoring system is an important infrastructure of power system. Once attacked, it will have a great impact on the country and society. Effective safety risk assessment of power monitoring system is helpful to timely risk control and safety management and avoid disasters.

At present, the evaluation of power system mainly focuses on power equipment or transmission network, and there is little research on power monitoring system. It is found that industrial control system and power monitoring system have certain similarities in structure and function, so its risk assessment method can be used as a reference for power monitoring system. There are many studies on risk assessment of industrial control system. In recent years, analytic hierarchy process (AHP) is widely used. For example, Song Y[1] and others use AHP to obtain the weight of each index in the hierarchical model, select relatively important indexes according to the comprehensive weight, and use BP neural network model to train to obtain the security level of the system; Xia Y[2] and others established a system risk assessment model from the four aspects of assets, vulnerability, threats and security measures by using AHP, obtained the weight value of each security element of the system,
and introduced the weight ratio to obtain the overall score of the system; Lu H.K[3] and others established a hierarchical model from the four aspects of assets, threats, vulnerability and security measures, and obtained the security evaluation value of the system by using fuzzy analytic hierarchy process and anti fuzzification method; Zheng Y[4] and others used fuzzy analytic hierarchy process to complete the risk evaluation of industrial automation platform from the three aspects of system confidentiality, integrity and availability.

On the basis the study of predecessors, this paper proposes a risk assessment method of power monitoring system based on FAHP and CVSS. The security objectives of power monitoring system are divided into three security sub objectives: confidentiality, integrity and availability; When assigning the relative importance of each layer of elements, the fuzzy comprehensive evaluation method is introduced to overcome the difficulty of AHP in the consistency test of judgment matrix; Using CVSS to quantify the indicators of the evaluation layer can eliminate the influence of subjective factors in the evaluation process to a certain extent; Using the fuzzy evaluation set, the final evaluation results are comparable, and the fuzzy evaluation vector of the system is obtained; Finally, the fuzzy evaluation vector is defuzzied to obtain the safety evaluation value and risk level of the system.

2. Related technologies

2.1. CVSS
CVSS, the common vulnerability scoring system, is an open evaluation method used to evaluate the characteristics and impact of vulnerabilities. CVSS is composed of three evaluation index groups: base, temporary and environmental, as shown in Figure 1. Among them, the base metric group represents the long-standing essential vulnerability, which will not change with time and user environment; The temporal metric group represents the vulnerability that changes over time but does not change with the user environment; Environmental metric group indicates vulnerability directly related to user environment.

2.2. Fuzzy analytical hierarchy process
Analytic hierarchy process (AHP) combines quantitative analysis and qualitative analysis to effectively deal with complex decision-making problems[5]. The key of AHP analysis lies in the construction and consistency transformation of judgment matrix. However, it is very difficult to test whether the judgment matrix is consistent, and when the judgment matrix is inconsistent, adjusting the matrix elements to make it consistent requires multiple adjustments and tests. In order to avoid the above problems, this paper introduces fuzzy comprehensive evaluation method, which is combined with AHP to form fuzzy analytic hierarchy process (FAHP).

The analysis steps of FAHP are as follows:

![Figure 1. Metric group of CVSS 3.0](image)
Step 1. Constructing fuzzy complementary judgment matrix $A = (r_{ij})_{n \times n}$ by expert, $r_{ij}$ represents the relative importance of element $X_i$ and $X_j$ related to an element of the previous layer. The assignment method is shown in the Table 1.

| Scale | Explanation                      |
|-------|----------------------------------|
| 0.5   | $X_i$ is as important as $X_j$   |
| 0.6   | $X_i$ is a little more important than $X_j$ |
| 0.7   | $X_i$ is more important than $X_j$ |
| 0.8   | $X_i$ is much more important than $X_j$ |
| 0.9   | $X_i$ is extremely more important than $X_j$ |
| 0.1, 0.2, 0.3, 0.4 | Inverse comparison of $X_i$ and $X_j$ |

Step2. The matrix A is transformed according to formula (1) to construct the fuzzy consistency judgment matrix. $r_i$ and $r_j$ represent the sum of the corresponding row elements.

$$ f_{ij} = \frac{r_i - r_j}{2n} + 0.5 $$

(1)

Step3. The established fuzzy consistency judgment matrix is calculated according to formula (2), and the relative importance of each element is obtained.

$$ w_i = \frac{1}{n} - \frac{1}{2\alpha} + \frac{1}{n\alpha} \sum_{k=1}^{n} r_{ik}, i = 1, 2, ..., n $$

(2)

Among them, the parameters $\alpha$ shall meet $\alpha \geq \frac{n-1}{2}$, the smaller the $\alpha$, the greater the weight difference.

3. Risk assessment scheme based on FAHP and CVSS

3.1. Hierarchical modeling

In order to apply FAHP to risk assessment, it is necessary to establish a reasonable system level risk assessment model. According to information security technology standards(GB/T 20984-2007)[6], the goal of the CIA triplet of Confidentiality, Integrity and Availability is the basic element of information security. Therefore, this paper carries out the overall security evaluation of the system from these three aspects. Since the key equipment in the system will have a certain impact on the CIA triplet, which is the key factor affecting the system, the evaluation layer selects key equipment to evaluate the impact of these three attributes. Above all, the hierarchical risk analysis model established is shown in Figure 2.
In the figure, $V_1, V_2, V_3, \ldots$ are vulnerabilities in the key equipment, which serve as the basis for assigning the relative importance of the key equipment in the evaluation layer.

### 3.2 Importance judgment and assignment of each element

The process of constructing judgment matrix is easily affected by subjective factors. In order to reduce this influence, CVSS is introduced to score the vulnerabilities of key equipment of the system, which is used as the basis for constructing fuzzy judgment matrix. Through vulnerability scanning and other methods, find the vulnerabilities on key equipment, and use these vulnerabilities to evaluate the impact of equipment on system confidentiality, integrity and availability.

According to the CVSS specification, the base metric group measures the confidentiality impact, integrity impact and availability impact of vulnerabilities. This paper uses the mean value of confidentiality, integrity and availability impact score of device vulnerabilities to measure the impact of devices on system confidentiality, integrity and availability, and constructs the evaluation layer fuzzy judgment matrix based on these. The specific methods are as follows:

Suppose the confidentiality score of $n$ key equipment in the system is $S_1, S_2, \ldots, S_n$, and for confidentiality, the fuzzy judgment matrix of the importance of key equipment is $R_{a1} = (a_{ij})_{n \times n}$. $a_{ij}$ is the relative importance scale of key equipment $i$ compared with key equipment $j$, and the assignment method is shown in the table 2.

| Condition | $Si-Sj$ | $a_{ij}$ |
|-----------|---------|----------|
| $Si>Sj$   | 0.42-0.56 | 0.9 |
|           | 0.28-0.42 | 0.8 |
|           | 0.14-0.28 | 0.7 |
|           | 0-0.14    | 0.6 |
| $Si=Sj$   | 0        | 0.5 |
| $Si<Sj$   | 0-0.14   | 0.4 |
|           | 0.14-0.28 | 0.3 |
|           | 0.28-0.42 | 0.2 |
|           | 0.42-0.56 | 0.1 |

According to the above method, the integrity fuzzy judgment matrix $R_{a2}$ and availability fuzzy judgment matrix $R_{a3}$ can be obtained. Then, according to the possible influence of the security
attribute layer on the system security evaluation value of the target layer and the relative importance of each attribute, the fuzzy judgment matrix $R_S$ is constructed.

3.3. Consistency conversion and calculation of weight value at each level
Using the method in section 2.2 to perform consistency conversion and calculation sorting on the judgment matrix $R_{a1}, R_{a2}, R_{a3}, R_{a4}$ constructed in the above steps, the weight subset of the importance of each index in the confidentiality, integrity, availability and system security evaluation value are $W_{a1}, W_{a2}, W_{a3}$ and $W_S$.

3.4. Establish fuzzy evaluation matrix for system equipment level
In order to make the final evaluation results comparable, a unified evaluation set is used for each index. Fuzzy evaluation is carried out on the indexes of key equipment in the hierarchical model. The method is as follows:

Suppose the influence degree of key equipment on system confidentiality is expressed as \{Very low, Low, Medium, High, Very high\}. Take "Key Equipment 1" in "Confidentiality" as an example, if 5% of personnel think that the impact of key equipment 1 on confidentiality is "Very low", 5% think that is "Low", 40% think that is "Medium", 30% think that is "High", and 20% think that is "Very high". Then, the evaluation membership vector of "Key Equipment 1" is $E_{a1} = (0.05, 0.05, 0.4, 0.3, 0.2)$. Similarly, the evaluation membership vector of other equipment in "Confidentiality" are $E_{a1}, E_{a2}, ..., E_{a4}$. Then the security evaluation membership matrix of confidentiality is obtained as: $E_s = [E_{a1}, E_{a2}, ..., E_{a4}]^T$.

According to formula (1), the fuzzy evaluation vector of computer confidentiality is as follows:

$$V_{a1} = W_{a1} \cdot E_{a1}$$

Similarly, we can get the fuzzy evaluation vectors of integrity and availability: $V_{a2}$ and $V_{a3}$.

Next, the fuzzy evaluation matrix composed of fuzzy evaluation vectors of various properties of the system is: $E_s = [V_{a1}, V_{a2}, V_{a3}]^T$.

Finally, the total system safety fuzzy evaluation vector is obtained from the following formula:

$$V_s = W_s \cdot E_s$$

3.5. Anti fuzzy transformation of comprehensive evaluation results
The result $V_s$ obtained in the above steps is a fuzzy vector, and the result of system risk assessment is still not clear enough. Therefore, it is necessary to defuzzify the result to make the result more accurate. The method is as follows:

The risk level of the system is divided into five levels and assigned. The set is expressed as $E = \{\text{Very safe, Relatively safe, Basically safe, Relatively dangerous, Very dangerous}\} = \{v_1, v_2, v_3, v_4, v_5\}$. The fuzzy evaluation vector $V_s = (s_1, s_2, ..., s_n)$ is defuzzified by formula (3), and then the safety level of the system is obtained.

$$S = \frac{\sum_{i=1}^{n} s_i v_i}{\sum_{i=1}^{n} s_i}$$

4. Example demonstration
The networking structure diagram of a power monitoring system is shown in the figure 3. This power monitoring system is divided into three layers: master station layer, network communication layer and equipment layer. The field equipment layer is not the target of network attack because the attack cost
is large and the benefit is small; However, once the network communication layer and master station layer are attacked, the data and control instructions will not be transmitted in time, which may lead to the collapse of power system. Therefore, the risk assessment in this paper is mainly aimed at the master station layer and network communication layer. The key equipment include monitoring terminal, application server, data server, Ethernet switch, data collector, PLC and other DCS systems. According to the above analysis, the established hierarchical risk assessment model is shown in the figure 4.

![Hierarchical modeling of power monitoring system](image)

Find the vulnerabilities on each key device through vulnerability scanning and score them by CVSS. For example, the main vulnerability list corresponding to the monitoring terminal and the confidentiality, integrity and availability scores of CVSS are shown in Table 3:

| Number of CVE | Confidentiality score | Integrity score | Availability score |
|---------------|-----------------------|----------------|------------------|
| CVE-2020-12011| 0.56                  | 0.56           | 0.56             |
| CVE-2020-10607| 0.56                  | 0.56           | 0.56             |
| CVE-2020-12028| 0.56                  | 0.56           | 0                |
According to the table, the impact scores of confidentiality, integrity and availability of the monitoring terminal are 0.3271, 0.2714 and 0.2957. Similarly, the confidentiality, integrity and availability scores of other key equipment can be obtained. The confidentiality scores of all equipment are as follows:

| Equipment                | Confidentiality score |
|--------------------------|-----------------------|
| Monitoring Terminal      | 0.3622                |
| Application Server       | 0.1553                |
| Data Server              | 0.2637                |
| Ethernet Switch          | 0.4730                |
| Data Collector           | 0.2362                |
| PLC                      | 0.5600                |
| Other DCS Systems        | 0.1593                |

According to the assignment method in Table 2, the obtained fuzzy judgment matrix of confidentiality is as follows:

\[
R_{c_i} = \begin{bmatrix}
0.5 & 0.7 & 0.6 & 0.4 & 0.6 & 0.3 & 0.7 \\
0.3 & 0.5 & 0.4 & 0.2 & 0.4 & 0.2 & 0.4 \\
0.4 & 0.6 & 0.5 & 0.3 & 0.4 & 0.2 & 0.6 \\
0.6 & 0.8 & 0.7 & 0.5 & 0.7 & 0.4 & 0.8 \\
0.4 & 0.6 & 0.6 & 0.3 & 0.5 & 0.2 & 0.6 \\
0.7 & 0.8 & 0.8 & 0.6 & 0.8 & 0.5 & 0.8 \\
0.3 & 0.6 & 0.4 & 0.2 & 0.4 & 0.2 & 0.5
\end{bmatrix}
\] (6)

According to the method in section 2.2, the influence weight vector of each key equipment on system confidentiality is: \( W_{ci} = (0.150, 0.117, 0.131, 0.166, 0.136, 0.179, 0.121) \). Similarly, the influence weight vectors \( W_{si} \) and \( W_{ai} \) of each equipment on system integrity and availability and the influence weight vector \( W_s \) of each safety element on the overall system can be obtained.

Through expert evaluation, the security evaluation membership matrix of confidentiality is obtained as follows:
According to formula (3), the fuzzy evaluation vector of confidentiality is:

\[ V_{a1} = W_{a1} \cdot E_{a1} = (0.0557, 0.1488, 0.3478, 0.2684, 0.1793) \]  

(8)

Similarly, \( V_{a2} \) and \( V_{a3} \) can be obtained.

Then the total fuzzy evaluation matrix \( E_{s} \) is:

\[
E_{s} = \begin{bmatrix}
V_{a1} \\
V_{a2} \\
V_{a3}
\end{bmatrix}
= \begin{bmatrix}
0.0557 & 0.1488 & 0.3478 & 0.2684 & 0.1793 \\
0.1182 & 0.0734 & 0.2278 & 0.326 & 0.2480 \\
0.3237 & 0.1349 & 0.2283 & 0.0754 & 0.2377
\end{bmatrix}
\]  

(9)

Finally, the safety fuzzy evaluation vector of the system is obtained from formula (4):

\[ V_{s} = W_{s} \cdot E_{s} = (0.1848, 0.1168, 0.2580, 0.2137, 0.2267) \]  

(10)

Make the comment set of system safety risk \( E = \{ \text{Very safe}, \text{Relatively safe}, \text{Basically safe}, \text{Relatively dangerous}, \text{Very dangerous} \} = \{1, 2, 3, 4, 5\} \), then the total system safety evaluation value is obtained according to formula (5):

\[ S = (0.1848 \times 1 + 0.1168 \times 2 + 0.2580 \times 3 + 0.2137 \times 4 + 0.2267 \times 5) / (0.1848 + 0.1168 + 0.2580 + 0.2137 + 0.2267) = 3.1807. \]

Since \( 3 < S < 4 \), the risk level of the system is between "Basic safe" and "Relatively dangerous". It can be seen that the system still needs to strengthen safety precautions and improve safety management level.

5. Conclusion

In order to avoid disasters in the high security threat environment, it is necessary to evaluate the risk of power monitoring system and carry out security management accordingly. Aiming at the risk assessment of power monitoring system, an assessment method based on fuzzy analytic hierarchy process and CVSS is proposed in this paper. Fuzzy consistency judgment matrix is introduced into analytic hierarchy process, which overcomes the shortcomings of traditional analytic hierarchy process; Using CVSS to quantify the indicators of the evaluation layer can eliminate the influence of subjective factors to a certain extent; Through the fuzzy comprehensive evaluation of the key equipment of the system, the comprehensive evaluation of the power monitoring system is completed from low to top, and the safety evaluation vector of the power monitoring system is obtained; By defuzzifying the safety evaluation vector, the accurate safety evaluation value and risk level of the system are obtained; Finally, an example is given to prove the rationality of this method, which can provide a basis for the safety management of power monitoring system. In the future work, we will refine the model of power monitoring system according to the actual situation, consider the vulnerability of management and personnel, and further reduce the influence of subjective factors in risk assessment methods.

Acknowledgments

Science and Technology Fund Project of State Grid Hebei Electric Power Co., Ltd: Development of special network security inspection toolbox for power monitoring system (Project No: kjcb2020-003)
References
[1] Song Y, Li Z.L, Chen M. (2020) A risk assessment method of industrial control system based on AHP-BP[J]. Network Security Technology and Application, 05:114-116.
[2] Xia Y, Gan J.J, Li L. (2019) Research on information security risk assessment method of industrial control system[J]. Automation Panorama, S2:58-60.
[3] Lu H.K, Chen D.Q, Peng Y, Wang Z.H. (2014) Quantitative Research on Risk Assessment for Information Security of Industrial Control System[J], Process Automation Instrumentation, 35(10):21-25.
[4] Zheng Y, Zheng S. (2015) Cyber Security Risk Assessment for Industrial Automation Platform, 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). Adelaide, SA.
[5] Wu W.G, Zhang Z.W, Wang Q.S. (2017) A Information Security Risk Assessment Model Based on AHP and Fuzzy Comprehensive Evaluation[J]. Journal of Chongqing University of Technology(Natural Science), 31(07):156-161.
[6] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China. GB/ T20984-2007 Information security technology-Risk assessment specification for information security[S]. Beijing: Standards Press of China, 2007.