Analysis of the Information Security Risk Assessment Mechanism Based on the Power System

Jian Li¹, Jia Wu¹, Yi Zhao²,*
¹State Grid Jibei Electric Power Co., Ltd, Hebei, China
²NARI Information & Communication Technology Co., Ltd, Nanjing, China

*Corresponding author e-mail: 16797174@qq.com

Abstract: In the risk assessment of the traditional power system information security, the traditional assessment methods are inefficient and the accuracy needs to be further improved. This paper establishes the analytic hierarchy process (AHP), designs a new information security risk assessment model in combination with fuzzy mathematics in risk assessment, and describes the content of the model in detail.

1. Introduction
At present, the power industry will produce a lot of data in the production and operation links. The power system is an important basic project in China, which is often faced with various threats in the construction links. However, the information security construction standard of the power system is not mature enough, and the information security risk assessment mechanism of the power system has not been completely established. Therefore, in the risk assessment link, its accuracy needs to be further improved.

2. Current Situation Analysis of Information Security Risk Assessment
Information security risk assessment is to improve the processing, transmission and storage of information and achieve the encryption of information on the basis of the application of relevant information technologies. Asset valuation is often threatened by security, therefore, it is necessary to analyze the content of security incidents, make reasonable judgments on the value of assets, and analyze the impact of security incidents on the whole organization.

In the process of assessing the security risk of the information system, it is necessary to improve the system risk assessment. The risk analysis is performed primarily in combination with assets, emerging threats, and security strategies. Risk analysis should also be combined with the nature of risk and assets. Threat analysis is to analyze the object of threat, and the attribute of assets mainly includes the value of assets. The attribute of vulnerability combines the blind spots in asset protection and the severity of asset damage.

In the process of information security assessment, international standards have also been made. In US computer system evaluation criteria, the computer security is divided into four levels, which combines integrity and confidentiality. China’s information security risk assessment issued relatively late. However, in recent years, China attaches great importance to this content. Now China has issued a lot of criteria, and the relevant evaluation mechanisms are becoming more and more standardized.
3. Related Concepts

3.1 The AHP Method

The AHP method is to analyze the goals and criteria, make decisions according to the way of analytic hierarchy process, and analyze the data qualitatively and quantitatively. The AHP method is used very frequently now, however, it has some shortcomings in the information security assessment of the power system. In the traditional risk assessment process, the evaluation method of qualitative analysis is relatively single, which only combines the unilateral experience of experts. However, there are great differences in the knowledge fields of various experts. If only the expert evaluation is adopted, the data information will not be comprehensive, and the accuracy of evaluation of various risk factors will also decrease. In the analysis of relevant assessment mechanisms, it is found that the AHP method combined with fuzzy mathematics can effectively improve the reliability of risk assessment.

3.2 Fuzzy Mathematics

The fuzzy mathematics can be used to analyze objects whose boundaries are not particularly clear in reality, and the fuzzy logic can be used to make the analysis of things more hierarchical. In the study of the information security risk assessment mechanism of the power system, the AHP method is applied, and the method of fuzzy data is also combined. In the process of system analysis, the hierarchical model is firstly established. According to the main content of risk assessment, the evaluation indexes meeting the practical application needs are established. The indexes are divided into three different levels. One is the target level, the other is the index level and the third is the specification level, so that the evaluation can be more objective and accurate.

In the same level, each factor can obtain a considerable weight, so that the relationship between each factor is closer, forming the subordinate relationship between the upper and lower levels. The lower factors play a good constraint effect on the upper factors.

Secondly, the way of triangular fuzzy mathematics complementary calculation matrix can be established. Combining the theory of fuzzy logic, the calculation matrix can be established.

Assuming there is a triangular fuzzy computing matrix, then the importance of each factor is compared, and the comparison relationship is calculated based on the experience of experts.

Thirdly, the fuzzy weight of single-layer factor is determined. In this link, the information of single-layer factor is analyzed, so as to calculate the objective weight.

Finally, combining with the formula, the compliance comparison matrix is established, and the matrix is established by combining the weight of each factor and the fuzzy value.

4. The AF-RA Risk Assessment Model

4.1 Risk Assessment and Quantitative Analysis

In the risk assessment, the security risk mechanism of the power system is analyzed quantitatively by combining the asset, vulnerability and threat.

(1) Core assets. In the process of core assets analysis, the evaluation project team should first investigate the relevant information, so as to obtain the information of the whole system and grasp the overall situation of the information. Secondly, the information is analyzed. By enumerating and dividing, the core asset information in the data is analyzed. In the overall asset information analysis, the evaluation of core assets should be improved to ensure that the types of assets are very clear, so as to conduct a detailed analysis of asset information.

In the application of information system, its main purpose is to improve the value of assets. In the process of increasing the value of assets, it is necessary to understand the attribution characteristics of assets, so as to fully understand the information of assets. In the process of asset evaluation, using the method of analytical hierarchy process, combined with the experience of industry experts, the attribution characteristics and the score of core assets are analyzed. According to the situation of the project group, three levels and triangular fuzzy mathematics are used to construct the matrix.

(2) Security threats. In the process of information security risk assessment of the power system, the key factor should be found. In the process of threat assessment and quantitative analysis, the main
threat points should be found, so as to improve the level analysis. According to the hierarchical structure of threat assessment, experts assign relevant probabilities and establish three different matrices.

(3) System vulnerability. In the solid-state characteristic analysis of information system core assets, vulnerability is often closely related to external risk factors. In the mandatory operation link, if the core assets are fluctuated, the assets will be unstable. In the information security risk assessment link of the power system, this factor is considered to be the most critical. The vulnerability of the system should be analyzed from two aspects of management and technology. The vulnerability includes not only physical layer and transport layer, but also application layer and management layer. In the process of project assessment, the information should be investigated according to the actual situation of power system, so as to list vulnerability. The schematic diagram of asymmetric current source method is shown in Fig.1.

![Schematic diagram of asymmetric current source method](image)

In the process of vulnerability level assessment, firstly, the vulnerability factors of the assessed objects should be analyzed to find out the vulnerabilities and analyze the severity of vulnerabilities. Secondly, it is necessary to assess the external impact faced by the assessed objects and assess what damage the threat has caused in vulnerabilities. Thirdly, according to the actual operation of the power system, each vulnerability is analyzed. With the help of analytic hierarchy process, the vulnerability is deeply analyzed, and the probability of vulnerability occurrence is accurately analyzed, and the experts evaluate it.

4.2 Risk Calculation

On the basis of the analysis of power system stability, it is necessary to combine the core assets, security threats, vulnerability and other characteristics to ensure that all hierarchical structures are interconnected and inseparable. In the structural framework of risk calculation, the safety value and risk parameters should be found by combining the analysis of assets and vulnerability, and the parameters should be calculated to find the risk factors of core assets, so as to evaluate the overall risk. Based on the combination of different risk factors and expert scoring information, the security risk parameters are analyzed by formula, and the risk set is found by combining multi-value data.
4.3 Determination of Risk Level

In the process of risk calculation, it is necessary to combine the risk data of various core assets, and rank the risks according to their importance. According to the analysis of risk assessment results and the safety application characteristics of the power system, the security risk level is processed to reduce the system vulnerability.

5. Conclusions

In this paper, according to the characteristics of the power system, combined with the security requirements, combined with fuzzy mathematics, the information security risk assessment mechanism is established, and the risk assessment model is improved.

References

[1] Z.Q. Liang, D.S. Lin, “Research on Information Security Risk Assessment Mechanism Based on Power System,” Information Network Security, vol.3, no.4, 2017, pp.86-90.
[2] X. Wang, T. Chen, J.Y. Zhang, etc., “Research and Application of Information Security Risk Assessment Technology in Power System,” Network Security Technology and Application, vol.6, no.4, 2013, pp.71-74.
[3] L.D. Chen, C.M. Lv, “Information Security Risk Assessment of Power System Based on Fuzzy Neural Network,” Hebei Electric Power Technology, vol.30, no.1, 2011, pp. 11-13.
[4] W. Ye, “Information Security Risk Assessment of Power System Based on Fuzzy Neural Network,” Network Security Technology and Application, vol.35, no.11, 2017, pp.125-127.
[5] Y.Q. Han, J. Guo, C.X. Guo, etc., “Security Risk Assessment of Information Physics Considering Software Failure Combined with Power System Intelligent Substation,” Journal of Electrical Engineering of China, vol.36, no.6, 2016, pp.1500-1508.
[6] K. Huang, “Discussion on Information Security Risk Assessment and Its Application in Power System,” Power Supply and Consumption, vol.7, no.5, 2007, pp. 27-30.
[7] J.Y. Chen, F. Yan, “Information Security Risk Identification of Urban Rail Transit Signaling System,” Urban FastRail Transit, vol.11, no.2, 2018, pp.119-123.