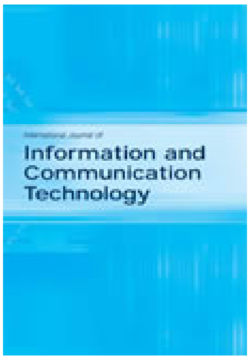


International Journal of Information and Communication Technology

ISSN online: 1741-8070 - ISSN print: 1466-6642
https://www.inderscience.com/ijict

Risk quantitative evaluation method of power communication network based on fuzzy analytic hierarchy process

Kaiyue An, Liyu Liu, Pengcheng Li

Article History:

Received:	09 September 2024
Last revised:	10 December 2024
Accepted:	11 December 2024
Published online:	25 February 2025

Risk quantitative evaluation method of power communication network based on fuzzy analytic hierarchy process

Kaiyue An*, Liyu Liu and Pengcheng Li

Communication Branch,
Inner Mongolia Electric Power (Group) Co., Ltd.,
Hohhot City, Inner Mongolia, China
Email: 1025136360@qq.com
Email: 394100789@qq.com
Email: 873489204@qq.com
*Corresponding author

Abstract: A quantitative risk assessment method for power communication networks based on fuzzy analytic hierarchy process (FAHP) has been proposed. Firstly, a risk indicator system is constructed using key performance indicators such as network reliability, security, latency, and bandwidth in power communication networks. Based on the risk indicator system, a fuzzy hierarchical structure model was established. The risk assessment results are transformed into specific quantitative values through quantitative analysis, in order to achieve quantitative evaluation of power communication network risks. After introducing this method, the frequency of these abnormal situations is effectively reduced and stabilised at four times or less per month, thereby enhancing the stability of the network; the accuracy of risk assessment within three months is consistently above 90%, with the highest reaching 97%; at 100 iterations, the risk assessment time of our method is only 7 seconds.

Keywords: fuzzy hierarchical analysis; electric power communication network; quantitative risk assessment; construction of risk index system; multi-level structure; fuzzy evaluation.

Reference to this paper should be made as follows: An, K., Liu, L. and Li, P. (2025) 'Risk quantitative evaluation method of power communication network based on fuzzy analytic hierarchy process', *Int. J. Information and Communication Technology*, Vol. 26, No. 4, pp.22–38.

Biographical notes: Kaiyue An is a Senior Engineer who graduated from Inner Mongolia University in 2015 with a Master's degree in Engineering, joined Inner Mongolia Electric Power Communication Company in September 2015, mainly engaged in communication technology research. She has published seven papers, authorised two invention patents, and won the title of 'Level 3 Engineer' in 2021.

Liyu Liu is an Engineer who graduated from University of Science and Technology Beijing in 2017 with a Master's degree in engineering, joined Inner Mongolia Electric Power Communication Company in July 2017, mainly engaged in communication technology research.

Pengcheng Li is an Engineer who graduated from Southwest Minzu University in 2014 with a master's bachelor in engineering, joined Inner Mongolia Electric Power Communication Company in January 2014, mainly engaged in communication technology research. He has published eight papers, and won the title of 'Level 3 Engineer' in 2021.

1 Introduction

Not only is the power communication network an essential part of the power system, but it is also essential to human survival. Ensuring the power system operates safely and steadily while increasing its overall efficiency is essential (Xiong and Chen, 2022). A quantitative risk assessment of the power communication network, which can be influenced by both internal and external factors, can be implemented to guarantee the steady operation of the power system, safeguard information security, and improve network performance (Wang et al., 2023).

In recent years, numerous scholars have explored various methods for quantitative risk assessment in power communication networks. For instance, Cai et al. (2022) proposed a new method for quantitatively evaluating these network risks. Through in-depth analysis of the complexity of power communication networks and the impact of various uncertainties on their secure operation, they have identified multidimensional operational risk probability indicators across different layers, including network service layer, topology layer, routing layer, device layer, and operation layer. Then, a multi state tree model is constructed using a sub node generation algorithm to capture all sub nodes of the state vector, thereby promoting quantitative risk assessment of the power communication network. However, when using the sub node generation algorithm to construct a multi state tree model, if the scale of the power communication network is large and there are many nodes and connections in the network, the multi state tree model may become extremely complex resulting in a decrease in evaluation efficiency. Wang et al. (2022) introduced an innovative method for quantitative risk assessment of power communication networks, which utilises convolutional neural networks to automatically extract key information from complex real-time datasets and combines support vector machines to identify and classify risks in these networks. This method can effectively detect potential security risks and take appropriate warning and response measures. However, when the dataset size of the power communication network is very large, the computational complexity of SVM will significantly increase. SVM needs to solve quadratic programming problems during the training process, which can be very time-consuming and consume a lot of computing resources for large-scale datasets. Mo and Wei (2022) proposed an alternative strategy based on fuzzy comprehensive evaluation method. They used the failure rate curve and Weibull distribution function in the power grid failure rate model to create a risk analysis model for communication link failures in the power grid. In order to comprehensively evaluate the risks of power communication network links, a fuzzy comprehensive evaluation method was adopted. By defining appropriate evaluation indicators and weights, integrating the impact of different factors, the overall risk assessment results are obtained. However, to use the failure rate curve and Weibull distribution function, it is necessary to fit the actual data. In the power communication network, obtaining accurate fault data is limited. If the data fitting is not accurate, it can lead to bias in the model's assessment of communication link failure risk, thereby affecting performance.

On the basis of the above research, a quantitative risk assessment method for power communication networks based on fuzzy analytic hierarchy process (FAHP) is proposed to address the shortcomings of the aforementioned technology. The research process of this method is as follows:

1 Construction of indicator system:

By conducting in-depth investigations and inspections of the power communication network, collecting and analysing relevant data, and selecting indicators from multiple dimensions such as voltage conditions, load conditions, and transient stability, a security index system for the power communication network is constructed.

2 Construction of fuzzy hierarchical structure model:

Based on the constructed power communication network security index system, a fuzzy hierarchical structure model (FAHP) is constructed using fuzzy mathematics theory. Firstly, construct a fuzzy comprehensive evaluation matrix to represent the relationship between the sets of safety indicators at all levels and the final set of risk assessment results. Then, by constructing and calculating the fuzzy reciprocal matrix and fuzzy consistency matrix, the relative weight of each risk indicator is obtained. Finally, the weight of each risk indicator is combined with its corresponding evaluation result level to obtain the risk assessment result of the entire network.

3 Comprehensive evaluation and quantitative analysis:

Finally, through quantitative analysis, the risk assessment results are transformed into specific quantitative values, providing strong support for risk management in power communication networks.

This method introduces fuzzy mathematics theory and constructs a fuzzy hierarchical structure model (FAHP) to quantitatively evaluate the risk of power communication networks. This method effectively solves the ambiguity and uncertainty in decision making and improves the accuracy and reliability of evaluation. By constructing a multi-level evaluation structure, the article allows for in-depth analysis of risk factors layer by layer and improves the subjectivity of weight calculation, making the evaluation results more objective. The experimental results show that the proposed method is highly consistent with the actual detection results for quantitative risk assessment of power communication networks; after introducing this method, the frequency of these abnormal situations was effectively reduced and stabilised at four times or less per month, thereby enhancing the stability of the network; the accuracy of risk assessment within three months is consistently above 90%, with the highest reaching 97%; at 100 iterations, the risk assessment time of our method is only 7 seconds.

The experimental verification provides strong technical support for the stable and secure operation of power communication networks, proving the ability to conduct efficient and accurate quantitative risk assessment of power communication networks (He et al., 2022). The research results of this article not only provide new ideas and methods for risk assessment of power communication networks, but also provide useful references and guidance for risk assessment in other fields.

2 Power communication network risk quantitative assessment

2.1 Security index system of power communication network

The most significant and important data was selected to act as the cornerstone for developing the security index system of the power communication network after a comprehensive investigation and examination of the network was carried out, along with a careful weighing of all the important data discovered there. The important information includes, but is not limited to, network response time, data transfer stability, information security protection capabilities, and network dependability. These indicators allow for a comprehensive assessment of the security performance of the power communication network, ensuring that the system can consistently and successfully operate even in the face of multiple potential threats.

2.1.1 Voltage conditions

One of the most important elements in the power communication network is voltage, which guarantees the stability of the power system. The following voltage-related indicators are assessed in this paper:

1 The fluctuation range of the load in the power communication network, i.e., the average active power margin of the nodes in the power system. A stable and sufficient power margin in the power system network can ensure that the system maintains a transient steady state when a sudden abnormal condition occurs (Zhang et al., 2022). The average active power margin is calculated and represented as

$$A_1 = 100\% \sum_{i=1}^{g} \alpha_{pi} / g \tag{1}$$

where α_{pi} represents the active power margin of a single node, which indicates the degree to which a single node can withstand sudden disturbances. The calculation process is shown in equation (2) (Fang et al., 2023).

$$\alpha_{pi} = \left(p_{limiti} - p_{0i} \right) / p_{0i} \tag{2}$$

In equation (2), p_{limiti} and p_{0i} represent the limit values of each node in the power communication network before an active power collapse and the power values during normal operation, respectively.

In equation (1), g represents the number of nodes in the power communication network with the first-grade active power margin, which is determined by the largest difference between the ascending order of the calculated node active power margin values. The g nodes before the largest difference are classified as the first grade. Since the weakness of the nodes determines the stability of the power communication network, setting $g \leq 10$ can significantly highlight the impact of active power margin on the power communication network.

2 During disturbances in the power communication network, if the system's reactive power margin is insufficient, the voltage may drop further, potentially leading to blackouts (Zheng et al., 2023). The average reactive power margin of nodes in the power communication network is represented as:

$$A_2 = 100\% \sum_{i=1}^{g} \alpha_{vi} / g \tag{3}$$

where α_{vi} represents the reactive power margin of a single node, indicating the degree to which a single node can withstand sudden disturbances. The calculation process is shown in equation (4) (Khan et al., 2024a).

$$\alpha_{vi} = \left(v_{limiti} - v_{0i}\right) / v_{0i} \tag{4}$$

In equation (4), v_{limiti} and v_{0i} represent the limit values of each node in the power communication network before a voltage collapse and the voltage values during normal operation, respectively. The setting of g is consistent with that in equation (1), with $g \leq 10$.

2.1.2 Load conditions

Load circumstances in a power communication network are an important factor in the network's safety, stability, and economic performance because they indicate the distribution state (Yang, 2023). The following load status indicators are examined in this paper:

1 Load rate: the ratio of the average load to the highest load in the power communication network is shown by this indication. The load distribution effect is better and the load rate is closer to 100% the higher the power communication network's utilisation rate. The load rate calculation formula is represented as

$$A_3 = 100\% \overline{P} / P_{\max} \tag{5}$$

where $\overline{P}$ and $P_{\max}$ represent the average load within a specific time period and the maximum load within the power communication network, respectively.

2 High load rate: in a power communication network, a high load rate is the proportion of lines that have a load that is higher than 70% of the maximum load relative to the total number of lines. High load rate lines may exceed load restrictions during power flow shifts in the power communication network, which could cause tripping and compromise network security. Equation (6) is the formula used to calculate the high load rate (Khan et al., 2024b).

$$A_4 = 100\% N_p / N_{sum} \tag{6}$$

where N_{sum} and N_p represent the total number of lines in the power communication network and the number of lines exceeding 70% of the maximum load, respectively.

2.1.3 Transient stability

In a power communication network, transient disturbances are common, and the system's ability to restore and stabilise its state is referred to as transient stability (Zheng, 2023). The transient stability indicators evaluated in this paper are as follows:

1 Critical clearing time: this is an evaluation indicator of transient stability in the power communication network, expressed as equation (7).

$$A_5 = 100\% t$$

where t represents the critical clearing time of the faulty line in the power communication network.

2 Average short-circuit overcurrent rate: equation (8) expresses this indication as the percentage difference between the rated current and the actual short-circuit current in the power communication network.

$$A_6 = 100\% \sum_{i=1}^{N_{sc}} I_i / N_{sc} \tag{8}$$

where N_{sc} and I_i represent the number of short-circuit lines and the overcurrent rate in the power communication network, respectively.

Through the construction of the power communication network security index system as described above, the final power communication network security index vector is obtained as $A = [A_1, A_2, A_3, A_4, A_5, A_6]$.

2.2 Construction of the fuzzy hierarchical structure model

Based on the risk index system constructed in Section 2.1, a fuzzy hierarchical structure model is established. This model decomposes the problem into hierarchical levels through a fuzzy comprehensive evaluation matrix.

The innovation of the power communication network risk quantitative assessment method, based on the FAHP, lies in its introduction of fuzzy mathematics theory, which effectively addresses the fuzziness and uncertainty in decision-making judgements, thereby enhancing the accuracy and reliability of the assessment. This method constructs a multi-level evaluation structure, allowing for a thorough analysis of risk factors layer by layer, while also improving the subjectivity of weight calculation, making the evaluation results more objective. Additionally, the FAHP method can flexibly integrate with other risk assessment techniques to build a comprehensive evaluation model, taking into account various risk factors comprehensively. This approach enhances the completeness and depth of the assessment, meeting diverse evaluation needs, and demonstrates its innovative value and practical potential in the field of power communication network risk management. The specific construction process is as follows:

2.2.1 Fuzzy comprehensive evaluation matrix

The fuzzy comprehensive evaluation matrix is used to represent the relationship between the sets of safety indicators at all levels and the final set of risk assessment results for the power communication network. In the two-layer structural model, each safety indicator is associated with one or more risk assessment result levels. This relationship is represented by the elements in the fuzzy comprehensive evaluation matrix, which reflect the degree of correlation between indicators and levels (Li et al., 2023). The fuzzy comprehensive evaluation matrix for the abnormal risk of the second level power system is represented by equation (9) (Mehmood et al., 2024):

$$C_1 = \begin{bmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} \\ c_{31} & c_{32} & c_{33} & c_{34} & c_{35} \\ c_{41} & c_{42} & c_{43} & c_{44} & c_{45} \\ c_{51} & c_{52} & c_{53} & c_{54} & c_{55} \\ c_{61} & c_{62} & c_{63} & c_{64} & c_{65} \end{bmatrix} \tag{9}$$

where c_{ij} represents the degree of relationship between factor A_i in the power communication network security index set and the risk assessment result grade B_j. The power communication network security index set includes six evaluation factors and five risk grades, so $i = 1, 2, 3, 4, 5, 6$ and $j = 1, 2, 3, 4, 5$.

Each row satisfies the normalisation condition, ensuring that the sum of membership degrees of each risk indicator at all possible evaluation result levels is 1, which can make the comparison between different indicators more fair and accurate. As shown in equation (10):

$$\sum_{j=1}^{5} c_{ij}, \qquad i = 1, 2, 3, 4, 5, 6 \tag{10}$$

Other fuzzy evaluation matrices are derived similarly.

2.2.2 Fuzzy consistent matrix and weight calculation

Fuzzy consensus matrix is used to calculate the weights of risk factors in power communication networks (Li et al., 2022). The following is the principle of weight calculation:

1 Fuzzy reciprocal matrix is used to represent the relative importance between different risk indicators. By comparing the importance of two indicators under specific conditions, this matrix can be constructed. This step is the foundation of weight calculation. Construct a fuzzy reciprocal matrix represented as equation (11):

$$C = \left(A_{ij}\right)_{n\times n} \tag{11}$$

where the relative importance of risk indicator A_i at i and risk indicator A_j at j is indicated by A_{ij}. The following situations may occur:

a if $A_{ij} = 0$, A_i and A_j are equally important

b if $A_{ij} < \frac{1}{2}$, A_j is more important than A_i; the smaller the value of A_{ij}, the higher the importance of A_j

c if $A_{ij} > \frac{1}{2}$, A_i is more important than A_j the larger the value of A_{ij}, the higher the importance of A_i.

2 Obtaining fuzzy consistent matrix: due to the lack of consistency in fuzzy reciprocal matrices, it is necessary to transform them into fuzzy consistent matrices through mathematical transformations. This step ensures that the elements in the matrix meet consistency requirements, providing a reliable foundation for subsequent weight calculations. This involves deriving a consistent matrix from a fuzzy reciprocal matrix lacking consistency by summing the matrices, as shown in equation (12):

$$c_i = \sum_{k=1}^{n} A_{ik}, \qquad (i = 1, 2, \ldots, k, \ldots, n) \tag{12}$$

A mathematical transformation is then applied to the result of equation (12) as shown in equation (13).

$$c_{ij} \left(c_i - c_j\right) / 2n + \frac{1}{2} \tag{13}$$

The matrix constructed through the process in equation (13) is the fuzzy consistent matrix *C*.

3 Normalise the rows of the fuzzy consistent matrix: normalisation is the process of converting the elements in the fuzzy consistent matrix into weight vectors. By normalising each row, the relative weight of each risk indicator can be obtained. These weights reflect the importance of different indicators in the evaluation. The weight vector $(\omega_1, \omega_2, \ldots, \omega_n)^T$ is obtained by normalising each row of the fuzzy consistent matrix *C* derived in step 2. The weight vector satisfies equation (14):

$$\omega_i = \left(\sum_{j=1}^{n} A_{ij} - 1 + n/2 \right) \Big/ [n(n-1)] \tag{14}$$

4 Calculate relative weights: after obtaining the relative weights of each risk indicator, it is necessary to calculate their importance relative to the target layer. This process starts from the target layer and calculates downwards layer by layer until reaching the lowest level of risk indicators. In this way, the weight vectors of all risk indicators relative to the target layer can be obtained (Zhu et al., 2022).

Let $a_1, a_2, \ldots, a_m$ represent the risk index at the next layer $X + 1$ of the top layer X of the power communication network, corresponding to the weight $\omega_{a_1}, \omega_{a_2}, \ldots, \omega_{a_m}$. At layer $X + 2$, the risk indices of the power communication network are represented by $a_1', a_2', \ldots, a_q'$. The weights of all risk indices in the power communication network at this layer are calculated using step (3), and the corresponding weight is represented as $\omega_{a_1'}, \omega_{a_2'}, \ldots, \omega_{a_q'}$. Thus, the weight vector of layer $X + 2$ relative to layer X is expressed as:

$$\omega_j^T = \sum_{i=1}^{n} \omega_{a_i} \omega_{a'_{ij}} \tag{15}$$

where $j = 1, 2, \ldots, n$. This process continues layer by layer until the lowest layer is reached. Finally, the importance of all risk indices in the power communication network relative to the target layer X is obtained, and the risk indices are ranked based on the results (Sun and Cai, 2022).

2.2.3 Comprehensive evaluation

After obtaining the weights of all risk indicators, use a fuzzy comprehensive evaluation matrix to assess the risks of the power communication network. This matrix combines the weight of each risk indicator with its corresponding evaluation result level to obtain the risk assessment result of the entire network. The obtained ranking results are used for the comprehensive evaluation of the risk assessment result set for each power communication network, yielding the matrix B_1, B_2, …, B_r. The fuzzy comprehensive evaluation matrix is then expressed as equation (16):

$$C = \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_r \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rs} \end{bmatrix} \tag{16}$$

Finally, the comprehensive evaluation matrix is transformed into the final risk assessment result through fuzzy transformation. The fuzzy transformation is expressed as equation (17):

$$B = A \cdot C \tag{17}$$

Equation (17) can be utilised to acquire the risk indicator evaluation outcomes within the power communication network.

2.3 Quantitative assessment of power communication network risk levels

Based on the risk index evaluation results obtained in Section 2.2, a comprehensive calculation is performed with the power communication network risk quantification vector (Wu et al., 2022), expressed as equation (18):

$$\varepsilon = \sum_{i=1}^{n} B_i D_i \bigg/ \sum_{i=1}^{n} B_i \tag{18}$$

where ε, B and D represent the power communication network risk quantification value, the fuzzy comprehensive evaluation result, and the risk quantification vector, respectively.

In the quantitative assessment of power communication network risk, the quantitative indicators are expressed in interval form. Therefore, the following relationships hold:

$$\varepsilon_{up} = \sum_{i=1}^{n} B_i D_{iup} \Big/ \sum_{i=1}^{n} B_i \tag{19}$$

$$\varepsilon_{down} = \sum_{i=1}^{n} B_i D_{idown} \Big/ \sum_{i=1}^{n} B_i \tag{20}$$

where D_{iup} and D_{idown} represent the upper and lower bounds of the risk quantification range in the power communication network, respectively.

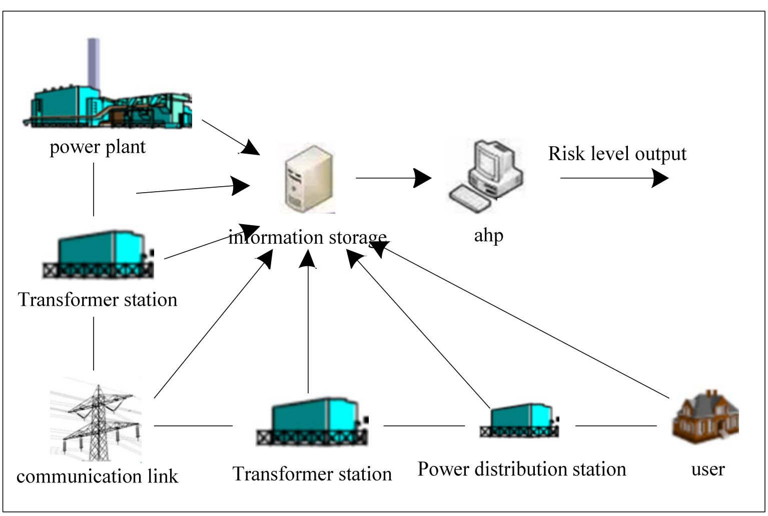
The interval range (ε_{down}, ε_{up}) obtained through equations (19) and (20) allows for the evaluation of abnormal conditions within the power communication network, thereby enabling the further quantitative assessment of risk levels.

3 Experiment

3.1 Experimental setup

An experiment was conducted to verify the effectiveness of the methodology proposed in this study for the quantitative risk assessment of power communication networks, using the test object being the power communication network of a regional power grid operator. Numerous data centres, power plants, substations, and the communication lines that link these crucial nodes make up this network. The scenario diagram for this experimental power grid company's quantitative assessment of power communication network risk is shown in Figure 1.

Figure 1 Scenario diagram of power communication network risk quantitative assessment (see online version for colours)



The power communication network risk assessment was conducted by the experimental power grid company using the scenario depicted in Figure 1. Table 1 enumerates the precise dimensions and pertinent parameters of this experimental power grid company.

Table 1 Relevant parameters of the experimental power grid company

Technical parameter	*Detailed value*
Number of power plants	3
Power plant capacity (MW)	800
Number of substations	10
Substation capacity (MVA)	200
Substation data transmission volume (TB/H)	2
Network bandwidth rate (Gbps)	1
Data centre processing speed (TB/H)	10
Power line communication transmission rate (Kbps)	1–14,000
Communication link transmission distance (m)	20–20,000

Obtain operational data from the monitoring system of each power plant, including the operating status of the units (such as whether they are operating normally, whether they are in maintenance status, etc.), power generation, equipment temperature, and other parameters. These data can reflect the operational stability of power plants and are an important basis for evaluating the risks of power communication networks. Real time monitoring data of equipment is obtained through sensors in the substation, such as oil temperature, voltage, current and other parameters of transformers, as well as status information of circuit breakers, isolating switches and other equipment. A total of 3,000 pieces of data were extracted, which were divided into training and testing sets according to a 7:3 ratio for experimental analysis. And the methods of Cai et al. (2022), Wang et al. (2022) and Mo and Wei (2022) were selected as comparative methods for performance testing.

3.2 Experimental indicators

1 Risk assessment indicators

According to the proposed method, risk levels are divided into multiple levels (such as levels 1 to 5), each corresponding to different consequences and response measures. This indicator describes the potential consequences of each risk level, which provide decision makers with intuitive information about the severity of the risk.

2 Actual testing indicators

This indicator is used to verify the accuracy of risk assessment. Experimenters evaluate the effectiveness of risk assessment methods by detecting abnormal situations in power communication networks and comparing them with risk assessment results.

3 Average transmission efficiency

This indicator is used to measure the data transmission capability of power communication networks. The experiment evaluates the effectiveness of the recommendation method in improving network performance by comparing the average transmission efficiency before and after its application. The improvement of average transmission efficiency means that the network can more effectively meet the data transmission requirements of the power system.

4 Accuracy of risk assessment

The accuracy of risk assessment can be measured by comparing the difference between actual risk and assessed risk. The expression is:

$$A = \left(1 - \frac{|F_p - F_s|}{F_s}\right) \times 100\% \tag{20}$$

Among them, F_s and F_p respectively represent actual risk and assessed risk.

3.3 Experimental results and analysis

The functioning of the experimental power grid company was assessed for risk throughout a month in order to confirm the efficacy of the quantitative risk assessment of the power communication network using the suggested method. Actual detection was used to validate the risk assessment's findings, and Table 2 displays the results of that particular comparison.

Table 2 Specific risk assessment results

No.	*Date/ time*	*Risk level assessed by proposed method*	*Corresponding consequence*	*Actual detection*	*Consistency*
1	3/2 8:16:52	Level 1	Negligible consequence, no action needed	Slight increase in network latency	Yes
2	3/4 18:38:16	Level 2	Minor consequence, appropriate action can be taken	Partial port failure	Yes
3	3/6 21:03:39	Level 1	Negligible consequence, no action needed	Electromagnetic pulse interference from lightning	Yes
4	3/8 6:23:27	Level 2	Minor consequence, appropriate action can be taken	Low-intensity malicious traffic	Yes
5	3/8 22:11:09	Level 1	Negligible consequence, no action needed	Packet loss	Yes
6	3/9 14:28:15	Level 2	Minor consequence, appropriate action can be taken	Low-intensity malicious traffic	Yes
7	3/12 17:01:39	Level 3	Serious consequence, appropriate action needed	IP address conflict	Yes
8	3/14 15:17:16	Level 2	Minor consequence, appropriate action can be taken	Partial port failure	Yes

Table 2 Specific risk assessment results (continued)

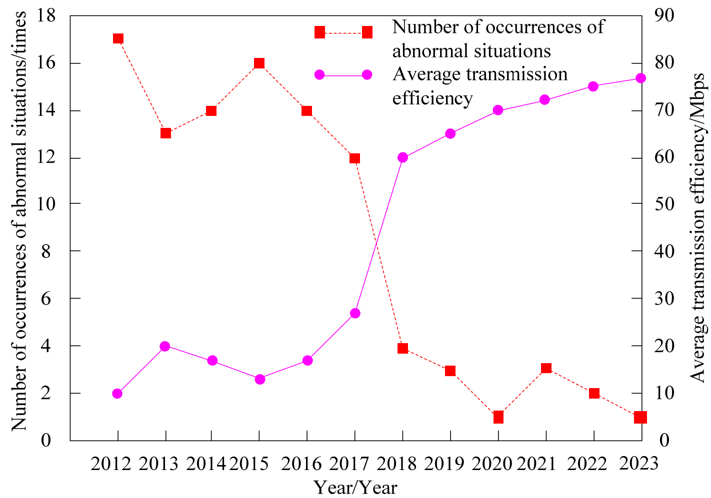
No.	*Date/ time*	*Risk level assessed by proposed method*	*Corresponding consequence*	*Actual detection*	*Consistency*
9	3/15 3:56:45	Level 1	Negligible consequence, no action needed	Slight increase in network latency	Yes
10	3/17 9:06:17	Level 5	Catastrophic consequence, must be resolved	Core server failure, network outage	Yes
11	3/17 13:14:34	Level 2	Minor consequence, appropriate action can be taken	Low-intensity malicious traffic	Yes
12	3/21 4:03:27	Level 1	Negligible consequence, no action needed	Packet loss	Yes
13	3/25 12:05:42	Level 2	Minor consequence, appropriate action can be taken	Low-intensity malicious traffic	Yes
14	3/25 14:05:14	Level 1	Negligible consequence, no action needed	Slight increase in network latency	Yes
15	3/29 6:11:34	Level 3	Serious consequence, appropriate action needed	Sensitive information was illegally accessed	Yes

The suggested method's quantitative risk assessment of the power communication network is in excellent agreement with the actual detection results, as demonstrated in Table 2. Strong validity and accuracy are demonstrated by the risk assessment's ability to correctly identify anomalous conditions in the power communication network. Communication breakdowns, equipment problems, and security risks are a few examples of these anomalous circumstances that could compromise the power system's ability to operate steadily. With great practical significance and application value, the risk assessment utilising the suggested method therefore offers solid support for the power communication network's safe, steady, and effective operation.

To validate the effectiveness of the proposed method for assessing the quantitative risk of power communication networks, a statistical comparison between the average transmission efficiency and the frequency of anomalous conditions over the preceding twelve years was carried out. The recommended course of action was followed for the last six years, but not for the first six. A comparison of the power communication network conditions before and after the recommended method was applied is shown in Figure 2.

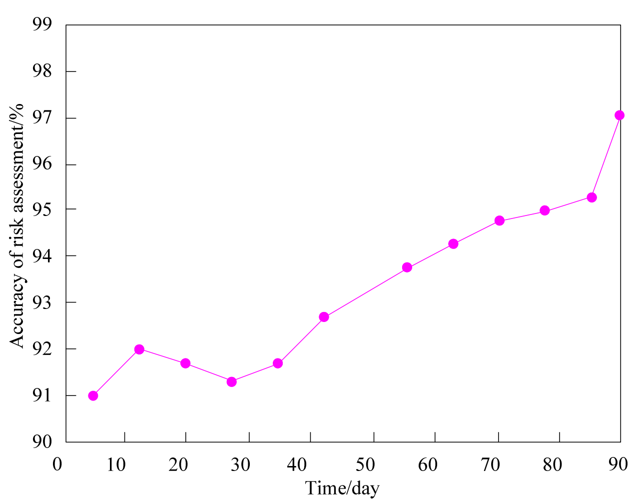
As illustrated in Figure 2, there is a marked improvement in the condition of the power communication network after implementing the proposed method. Prior to its application, the monthly frequency of abnormal conditions in the network consistently exceeded 10, significantly affecting the network's stability and safety. However, following the introduction of the method, the frequency of these abnormal conditions was effectively reduced, stabilising at 4 or fewer occurrences per month, thereby enhancing the network's stability. As a result, the average transmission efficiency of the power communication network improved from 10–30 Mbps to 60–80 Mbps. This increase in data transmission speed more effectively meets the power system's data transmission requirements and provides robust support for the intelligent and efficient operation of the power system. These results confirm the effectiveness of the proposed method and suggest promising potential for the future development of power communication networks.

Figure 2 Comparison of conditions before and after using the proposed method (see online version for colours)



To further verify the practicality of the design method, practical application analysis and testing were conducted. The method was applied to the above-mentioned power grid company and operated for three months to test the accuracy of the power communication network risk assessment during this period. The results are shown in Figure 3.

Figure 3 Accuracy of power communication network risk evaluation (see online version for colours)



As shown in Figure 3, after implementing the proposed method, the accuracy of risk assessment within 3 months remained above 90%, with the highest reaching 97%. This indicates that the method proposed in this paper can effectively achieve quantitative risk assessment of power communication networks. This is because the article selected indicators such as network reliability, security, latency, and bandwidth as the cornerstone for developing a security indicator system for power communication networks through a comprehensive investigation and inspection of the power communication network. This provides a solid foundation for the subsequent fuzzy hierarchical structure model and effectively improved the performance of risk assessment.

To further verify the applicability of the design method, the methods of Cai et al. (2022), Wang et al. (2022) and Mo and Wei (2022) were selected as comparative methods for evaluating efficiency. The test results are shown in Table 3.

Table 3 Risk assessment time for four methods

Number of iterations (times)	*Cai et al.'s (2022) method (s)*	*Wang et al.'s (2022) method (s)*	*Mo and Wei's (2022) method (s)*	*This paper method (s)*
10	15	19	25	6
20	14	18	26	8
30	16	17	24	6
40	15	20	22	5
50	18	21	24	6
60	17	19	20	7
70	18	18	24	6
80	14	16	21	3
90	18	17	22	4
100	16	16	20	7

From Table 3, it can be seen that as the number of iterations increases, the risk assessment time of all four methods fluctuates, but the method proposed in this paper is significantly better in overall efficiency than the other three methods. For example, at 100 iterations, the risk assessment time of our method is 7 seconds, while the methods in Cai et al. (2022), Wang et al. (2022) and Mo and Wei (2022) require 16 seconds, 16 seconds, and 20 seconds, respectively. This indicates that the method proposed in this article demonstrates significant efficiency advantages in risk assessment of power communication networks, with much lower risk assessment time compared to the methods in Cai et al. (2022), Wang et al. (2022) and Mo and Wei (2022). Moreover, the method presented in this article demonstrates good stability at different iteration times, with minimal fluctuations in risk assessment time.

4 Conclusions

Quantitative risk assessment of power communication networks can effectively improve their stability and transmission efficiency. This is of great significance for the expansion of power communication networks. This study provides a quantitative risk assessment method for power communication networks based on the fuzzy analytic hierarchy process

(FAHP). This method constructs a power communication network security indicator system that includes key performance indicators such as network reliability, security, latency, and bandwidth, and establishes a fuzzy hierarchical structure model based on these indicators. Through the application of fuzzy mathematics theory, this method effectively solves the ambiguity and uncertainty in decision making, and improves the accuracy and reliability of risk assessment. The experimental verification results show that this method is not only highly consistent with the actual detection results, but also significantly reduces the frequency of network anomalies and enhances the stability of the network after introduction. In the risk assessment within three months, the accuracy was consistently above 90%, with the highest reaching 97%, demonstrating the efficiency and accuracy of this method. In summary, the method proposed in this study not only provides new ideas and methods for risk assessment of power communication networks, but also provides useful references and guidance for risk assessment in other fields.

Acknowledgements

Fund Project: Science and Technology Project of Inner Mongolia Electric Power (Group) Co., Ltd. (Project Name: Research and Application of Key Technologies for Multi-dimensional Risk Assessment and Early Warning of Power Communication Networks, Project Number: 2023-5-41)

References

Cai, W., Zhang, Y., Chen, L. et al. (2022) 'Probabilistic evaluation algorithm of power communication network operation risk based on multi state tree', *Microcomputer Applications*, Vol. 38, No. 5, pp.79–82.

Fang, H., Wu, L. and Zhou, H. (2023) 'Research on routing optimization algorithm of power communication network based on improved ant colony algorithm', *Electrical Measurement & Instrumentation*, Vol. 60, No. 5, pp.97–102.

He, D-q., Liu, G-q., Chen, Y-j. et al. (2022) 'Evaluation method of train communication network performance based on normal cloud model and fuzzy analytic hierarchy process', *Journal of Traffic and Transportation Engineering*, Vol. 22, No. 2, pp.310–320.

Khan, A.A., Chen, Y-L., Hajjej, F. et al. (2024a) 'Digital forensics for the socio-cyber world (DF-SCW): a novel framework for deepfake multimedia investigation on social media platforms', *Egyptian Informatics Journal*, Vol. 7, No. 1, p.27.

Khan, A.A., Laghari, A., Baqasah, A.M. et al. (2024b) 'ORAN-B5G: a next generation open radio access network architecture with machine learning for beyond 5G in Industrial 5.0', *IEEE Transactions on Green Communications and Networking*, Vol. 8, No. 3, p.1026–1036.

Li, Y., Yang, H., Cui, J. et al. (2022) 'Security and reliability analysis of D2D communication in electric power 5G network by using nearest location-based relay selection strategy', *Journal of Computer Applications*, Vol. 42, No. 2, pp.168–174.

Li, Y-p., Liu, F-h. and Zhan, H-q. (2023) 'Hierarchical proteus virtual simulation analysis of transient circuit', *Computer Simulation*, Vol. 40, No. 2, pp.498–502.

Mehmood, F., Khan, A.A. et al. (2024) 'BLPCA-Ledger: a lightweight plenum consensus protocols for consortium blockchain based on the hyperledger indy', *Computer Standards & Interfaces*, Vol. 25, No. 9, p.103.

Mo, L. and Wei, L. (2022) 'Risk assessment method for power grid communication link failure based on fuzzy comprehensive assessment', *Int. J. Internet Protoc. Technol.*, Vol. 15, No. 2, pp.69–75.

Sun, C. and Cai, L. (2022) 'Operation evaluation of distribution automation system based on fuzzy analytic hierarchy process', *Computer & Digital Engineering*, Vol. 50, No. 3, pp.503–507, 590.

Wang, N., Tian, J-y., Dong, N. et al. (2022) 'Real-time risk-assessment and early-warning technology of smart grid regulation system based on improved SVM', *Journal of Shenyang University of Technology*, Vol. 44, No. 1, pp.7–13.

Wang, Z., Shang, G., Wang, C., et al. (2023) 'Risk assessment and maintenance priority decisionmaking method for failure of subsystem of CODAS-based CBTC onboard system', *Journal of the China Railway Society*, Vol. 45, No. 8, pp.87–98.

Wu, Q., Wang, Y., Zeng, L., Sun, Y. et al. (2022) 'Communication technology planning for power terminal communication access networks in the '14th five-year plan' based on analytic hierarchy process', *Electric Power*, Vol. 55, No. 5, pp.174–181.

Xiong, W-X. and Chen, Y-G. (2022) 'Safety evaluation of railway communication system based on set pair extension and improved analytic hierarchy process', *Computer Systems & Applications*, Vol. 31, No. 2, pp.285–290.

Yang, S-y. (2023) 'Research on routing equalization method of power communication network based on SVM', *Information Technology*, Vol. 47, No. 4, pp.101–106.

Zhang, L., Ji, C., Wang, X. et al. (2022) 'A routing optimization strategy for an electric power communication network based on the minimum path selectivity degree', *Power System Protection and Control*, Vol. 50, No. 1, pp.141–147.

Zheng, M., Zhao, H., Rao, H. et al. (2023) 'Construction of transmission model of electric power SDH communication network based on gradient DPSO algorithm', *Automation & Instrumentation*, Vol. 2023, No. 9, pp.83–86, 91.

Zheng, X. (2023) 'Research on load balancing optimization strategy of power communication network based on improved Lagrange relaxation algorithm', *Electrical Measurement & Instrumentation*, Vol. 60, No. 4, pp.85–91.

Zhu, T., Xie, Y., Zhong, S. et al. (2022) 'Application of fuzzy analytic hierarchy process in selection of power grid operation schemes', *Electric Power*, Vol. 55, No. 8, pp.121–128.