Scientific Research Publishing

Journal of Computer and Communications, 2022, 10, 56-71
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Risk Assessment of Distributed Energy System Based on Fuzzy Analytic Hierarchy Process

Chunning Fu

School of Computer Science, University of Nottingham, Nottingham, UK
Email: fcn9694@163.com

How to cite this paper: Fu, C.N. (2022) Risk Assessment of Distributed Energy System Based on Fuzzy Analytic Hierarchy Process. *Journal of Computer and Communications*, **10**, 56-71.
https://doi.org/10.4236/jcc.2022.1011005

Received: April 19, 2022
Accepted: November 7, 2022
Published: November 10, 2022

Abstract

Risk assessment of distributed energy system often has uncertainty and subjective problems. The problems will have some impact on the results. To solve the problems, a method of improved fuzzy analytic hierarchy process is proposed. By using the fuzzy analytic hierarchy process method, a hierarchical analysis model is established. And then according to the given judgment matrix of each index layer, we calculate whether it meets the consistency condition. And then if the judgment matrix does not meet the consistency condition, the problem will be solved by the improving of particle swarm optimization (PSO) with Kalman filter. The practice in the distributed energy system shows that the method can not only fully reflect the fuzziness of assessment elements and process, but also reduce the influence of individual subjective factors and better evaluation results can be achieved.

Keywords

Fuzzy Theory, Analytic Hierarchy Process, Distributed Energy System, Risk Assessment

1. Introduction

The development of computer systems and the application of computer technology on different occasions have gradually increased, and more and more attacks have followed. Traditional protection methods take corresponding measures after the system is attacked, including passive protection methods such as firewalls, intrusion detection or white listing, and cannot detect and deal with the hazards in time. Therefore, effective risk assessment methods are used to discover the existence of the system in advance. For vulnerabilities and threats, it is very important to formulate scientific and effective security strategies and actively adopt security defenses. There is a certain amount of research on information security risk assessment at home and abroad. The standard policies, technical methods and organizational structure related to risk assessment require the establishment of national security agencies and authoritative institutions to ensure the credibility of the assessment process and assessment results.

Risk assessment is a scientific security assessment method. Through detailed assessment of assets, threats, and vulnerabilities, and assigning values to different degrees of security threats and vulnerabilities, the risk value is finally calculated, allowing users to intuitively understand the current security status of the system and take effective protective measures afterward. This method has been widely used in different industries and is the first and critical step to assess its security status. In the energy Internet environment, more information security issues are exposed, including certain risks in all aspects of production, transmission, and communication. To take scientific and effective protective measures, it appears to be an information security risk assessment for distributed energy systems. It is very necessary. The information system in the distributed energy network system architecture is a key link to ensure the correct transmission and message transmission. The risk assessment team established by the State Information Office has also formulated the "Information Security Risk Assessment Specification" [1] and "Information Security Risk Management "Guide" [2] provides standards and basis for my country's information security risk assessment work. According to the principles of evaluation, it can be divided into evaluation methods based on mathematical knowledge, evaluation methods based on game theory, and evaluation methods based on machine learning. For the special evaluation object of the distributed energy system, any threat that exists may become the target of attackers and cause a certain range of power system failures, which will seriously affect people's lives.

In the process of risk assessment, the assessment object should be analyzed from multiple angles. To reduce the possible impact of subjective factors or other irrelevant factors on the assignment of indicators, Yu *et al.* [3] used gray theory to calculate the risk matrix, and then used the network analysis method to calculate each risk factor and calculates its weight. This method reduces the influence of subjective factors of experts. Huang *et al.* [4] used fuzzy sets to improve traditional evidence theory and solved the BPA function to reduce the influence of subjective factors. The difficulty brought by Zhang *et al.* [5] used rough set theory to reduce the complexity of analysis, grasped key nodes in the evaluation process, eliminated factors that did not affect the evaluation results, discovered possible combination threats, and automatically Generate an evaluation model. To comprehensively evaluate the safety of the evaluation object from multiple angles, Han Xia *et al.* [6] used the analytic hierarchy process in the safety evaluation of the operation of the power system, by constructing an indicator system and calculating the weight of each indicator to assess the safety status of the system. With a clear understanding, Ren Qiujie *et al.* [7] used a combination of fuzzy hierarchy method and attack tree method to carry out an effective security assessment of the information system. The AHP method is widely used when dealing with multi-attribute decision-making problems by decomposing the final goal into multiple levels to calculate the weights respectively. However, because the judgment matrix is prone to unreasonable consistency, it is impossible to accurately obtain the weight of each indicator. The particle swarm method is often used to solve the problem of parameter optimization and multi-objective solution. Shang Wenli *et al.* optimized the parameters of the support vector machine by using the particle swarm optimization method and established a support vector machine anomaly detection model [8]. The KPSO method has a better improvement in convergence speed and accuracy based on the standard particle swarm method. Dai Shaowu *et al.* [9] used the improved KPSO method to obtain better results in acceleration calibration.

There are many kinds of swarm intelligence algorithms, including Ant Colony Optimization, Particle Swarm Optimization, Artificial Bee Colony Algorithm and and so on. The common features between them include the independence between individuals, using local and global information to interact.

As an earlier proposed algorithm, the PSO has the advantages of fast convergence, simple and low complexity in calculation. Compared with other swarm intelligence algorithms, it can be used to solve more problems and it is more applicable to the content of this article.

Therefore, the paper uses the improved particle swarm method to modify the judgment matrix that has not passed the consistency test and obtains the judgment matrix that best fits the actual situation and conforms to the consistency test. And then combines the analytic hierarchy process to obtain the final risk of the distributed energy system. The experiment proves that the revised result can better reflect the true weight of the indicator, which provides a reliable basis for the application of risk assessment.

2. Security Risk Assessment in Distributed Energy System

2.1. Distributed Energy System Structure

Natural gas distributed energy, as the current vigorous development direction, has the particularity of the interconnection and interoperability of energy, electricity, water and heat, and the network, making its risk assessment need to be more comprehensive and detailed. From the distributed energy system architecture shown in **Figure 1**, a complete distributed energy system includes six parts: energy supply, power transformation system, thermal energy conversion system, energy storage system, energy management system, and load side, which make full use of the area The various energy resources inside and the power system, the thermal system cooperate with the operation, and the intelligent management.

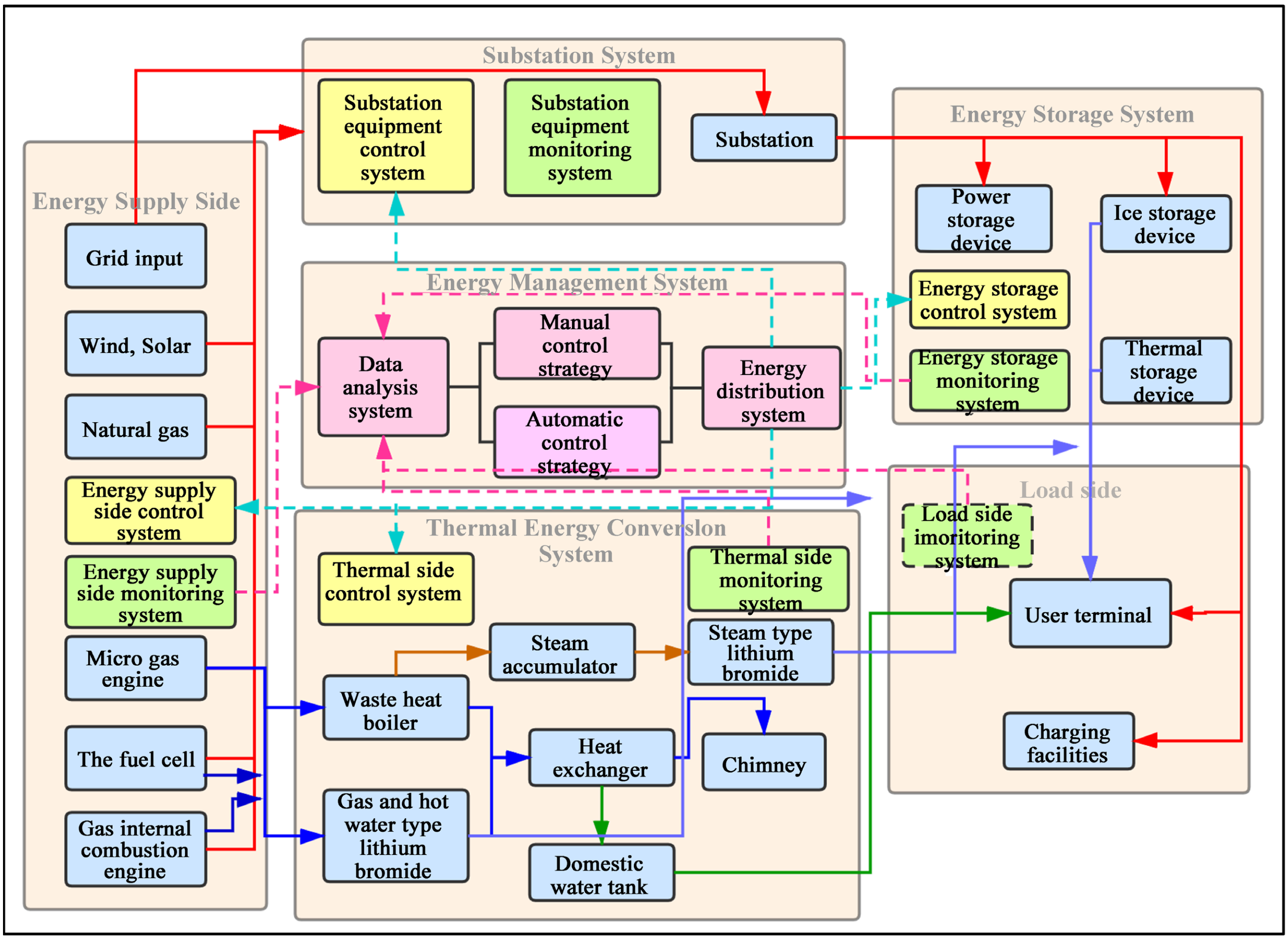

Substation System
Substation equipment control system
Substation equipment monitoring system
Substation
Energy Storage System
Power storage device
Ice storage device
Energy storage control system
Energy storage monitoring system
Thermal storage device
Energy Supply Side
Grid input
Wind, Solar
Natural gas
Energy supply side control system
Energy supply side monitoring system
Micro gas engine
The fuel cell
Gas internal combustion engine
Energy Management System
Data analysis system
Manual control strategy
Automatic control strategy
Energy distribution system
Load side
Load side imoritoring system
User terminal
Charging facilities
Thermal Energy Converslon System
Thermal side control system
Thermal side monitoring system
Steam accumulator
Steam type lithium bromide
Waste heat boiler
Heat exchanger
Chimney
Gas and hot water type lithium bromide
Domestic water tank

Figure 1. Distributed energy system structure.

2.2. Hierarchical Analysis Model

After identifying the elements of the system, a risk assessment index system was established according to the analytic hierarchy process, and assets, threats, vulnerabilities, and existing security measures were taken as four first-level indicators [10]. The assessment of assets is carried out from the three aspects of the three elements of information security. The assessment indicators of threats are carried out in two categories: environmental factors and human factors. The assessment of vulnerabilities mainly starts from the two perspectives of technology and management. Measures are evaluated in terms of preventive measures and protective measures. In summary, the evaluation index system established in this article has 3 first-level indicators, 7 second-level indicators, and 14 third-level indicators, as shown in Figure 2.

Risk assessment evaluates assets from three aspects: whether the data is leaked, whether it has been tampered with, and whether it can be used normally. The indicators that affect threats include environmental and human factors. Environmental factors refer to threats caused by force majeure and system environmental problems. Human factors mainly refer to potential threats such as man-made malicious manipulation of virus implantation. The impact indicators

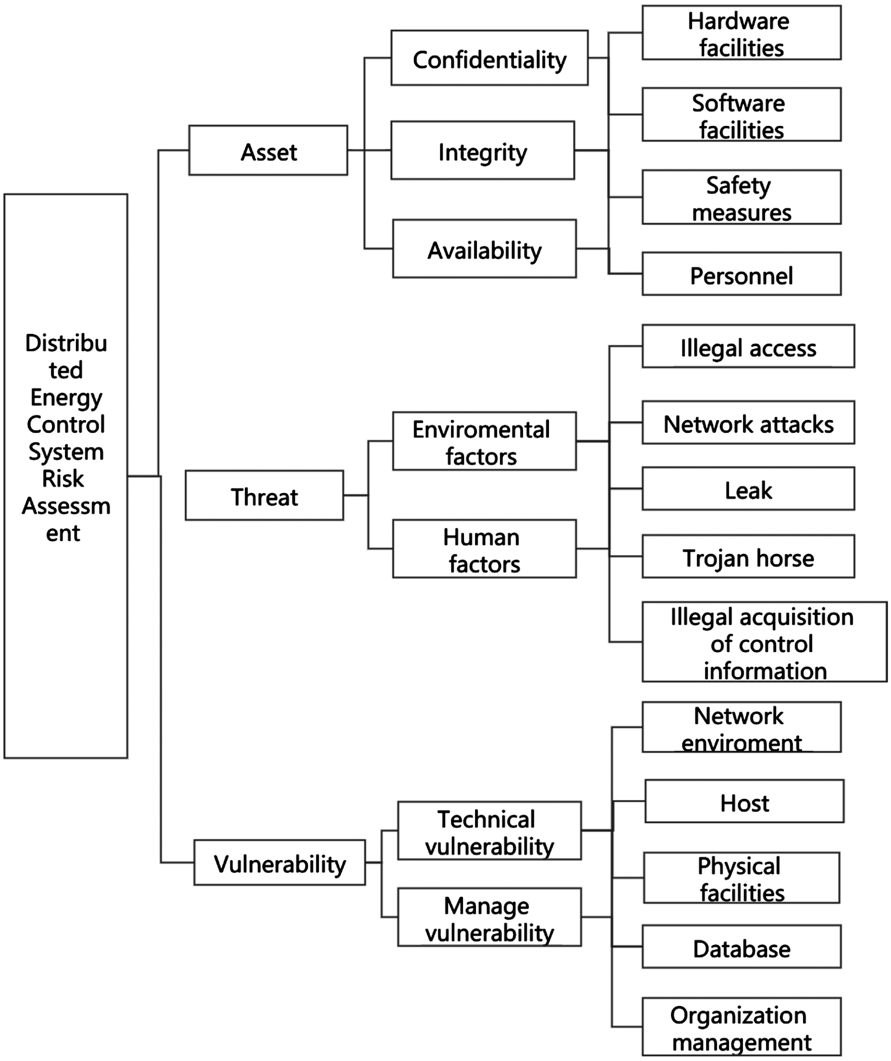


Figure 2. Hierarchical analysis model of distributed energy system.

on vulnerability are developed from two aspects: technology and management. Specifically, it refers to the design flaws of the system itself or the lack of advanced technology, and there may also be problems in the establishment and implementation of management regulations.

3. Risk Assessment Method

3.1. AHP Method

Analysis of Hierarchy Process (AHP) [11] as an effective evaluation method, its main analysis principle is to divide the problem to be analyzed into multiple levels, before each level according to the form of two-to-two comparison, Get the weight of each element on the layer, and finally sort them in a certain additive manner to get the total weight. The main steps are as follows:

1) Build a hierarchical model

The overall hierarchical structure model established in this paper is divided into four levels from top to bottom, and the indicators of each layer are related to the indicators of the previous layer. First, set up the general target problem to be solved, then put forward several aspects of the problem, and finally propose specific measures to solve each small problem.

2) Construct a judgment matrix

The judgment matrix reflects the importance of the elements at each level and is arranged in order, using the nine-point method for assignment. The judgment matrix can be as follows, where: $b_{ii} = 1$, $b_{ji} = 1/b_{ij}$.

$$B = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{bmatrix} \tag{1}$$

Then calculate the value of CI, $\text{CI} = \frac{\lambda_{\max} - n}{n-1}$, $\lambda_{\max}$ is the maximum eigenvalue of the matrix. If $\text{CR} = \frac{\text{CI}}{\text{RI}} < 0.1$, we think that the consistency of the matrix is better, otherwise you have to adjust the matrix with the following step (3) and step (4).

3) Hierarchical single sort

Find the eigenvector W of the matrix, and then normalize to get the weight value, as shown below.

$$W = (w_1, w_2, \cdots, w_n)^{\text{T}}, w_i = w_i^* \Big/ \sum_{i=1}^{n} w_i^* \tag{2}$$

4) Hierarchical total order

Calculate the weights from the top layer in order, and finally get the weight of the bottom layer compared to the top layer.

3.2. AHP Method Based on Fuzzy Theory

The analytic hierarchy process is prone to problems when there are many rating indicators. Therefore, this paper uses the fuzzy hierarchy method to solve the problem of consistency. The specific steps and processes are shown in Figure 3.

1) Establish a hierarchical structure: establish an evaluation hierarchy according to the risk assessment model and analytic hierarchy method, and then establish a corresponding analytic hierarchy model for assets, threats, and vulnerabilities.

2) Establish fuzzy complementary matrix: The construction of fuzzy complementary matrix $R = (a_{ij})_{n\times n}$ is produced by comparison between elements.

3) Fuzzy weight calculation of single-level factors: Calculate the number of

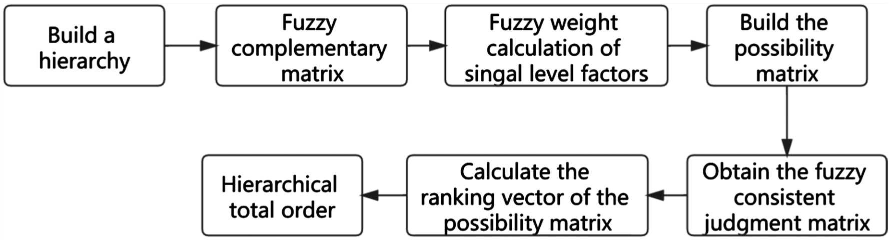

Build a hierarchy
Fuzzy complementary matrix
Fuzzy weight calculation of singal level factors
Build the possibility matrix
Obtain the fuzzy consistent judgment matrix
Calculate the ranking vector of the possibility matrix
Hierarchical total order

Figure 3. Flow chart of fuzzy hierarchy method.

fuzzy weights $\tilde{w}_i$, triangular fuzzy number $\tilde{a}_{ij}$, pessimistic estimates l_{ij}, possible estimates m_{ij} and optimistic estimates u_{ij}.

4) Establish the possibility matrix: Calculate the probability value *p*.

5) Find the fuzzy consistent judgment matrix: According to the possibility degree *p*, we can get the fuzzy consistent discriminant matrix *R*, $R=\left(r_{ij}\right)_{n\times n}$.

6) Calculate the ranking vector of the possible degree matrix: The ranking vector W is calculated from the complementary judgment matrix.

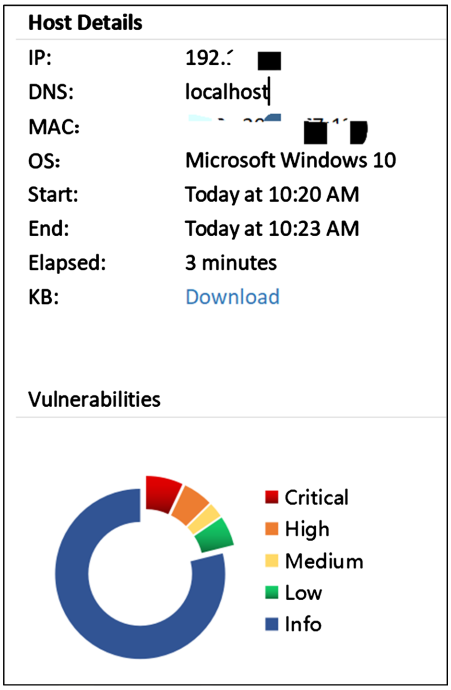
7) Level total sort: Calculate the weight of the index of the target layer.

4. Experiment Analysis

4.1. Evaluation Data Collection

To prove the effectiveness of the improved method for risk assessment, this paper establishes a small gas distributed energy system, and scans its assets, existing threats, and vulnerabilities through vulnerability scanning software and assessment tools, and uses this as a basis. Combine the relevant indicators of national risk assessment to construct an assessment data set. Using vulnerability scanning software to scan the host, it can be seen that there are many vulnerabilities in the system as shown in Figure 4, and the detailed information of the host is displayed at the same time. This also shows that there are many potential threats in the control system host. Key attention should be given to indicators when assigning values.

Besides, through the analysis and processing of 274,628 raw data in the natural gas control system data set, that is, the data set itself is divided into normal behavior data and abnormal behavior data using the label value. And data with a



Host Details

IP:	192.[redacted]
DNS:	localhost
MAC:	[redacted]
OS:	Microsoft Windows 10
Start:	Today at 10:20 AM
End:	Today at 10:23 AM
Elapsed:	3 minutes
KB:	Download

Vulnerabilities

Figure 4. Vulnerability scan information.

label value of 0 is divided into normal behavior data, data with a label value of 1 is classified as NMRI, data with a label value of 2 is classified as CMRI, data with a label value of 3 is classified as MSCI, data with a label value of 4 is classified as MPCI, and data with a label value of 5 is classified as MFCI, the data with a label value of 6 is classified as DoS, and the data with a label value of 7 is classified as reconnaissance, and then the database is used to perform statistics on various behavioral data. Including 214,580 normal behavior data and 60,048 abnormal behavior data, accounting for 78.13% and 21.87% of the total data volume respectively. The data is centralized. The specific percentages of various types of attacks are shown in Figure 5. It can be seen from Figure 5 that there are many different types of attack data in the natural gas control system. These attack behaviors will cause great harm to the security of the system, especially malicious parameter command injection attacks and complex malicious response injection attacks. It should be focused on during the evaluation process.

Then use the security risk assessment software to scan the system and calculate the corresponding evaluation index weights. As a simple assistant software

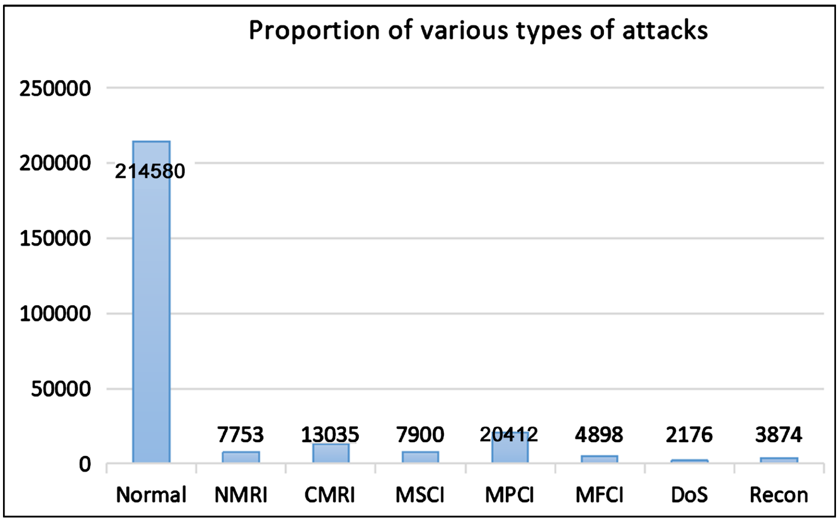


Figure 5. Percentage of offensive behavior.

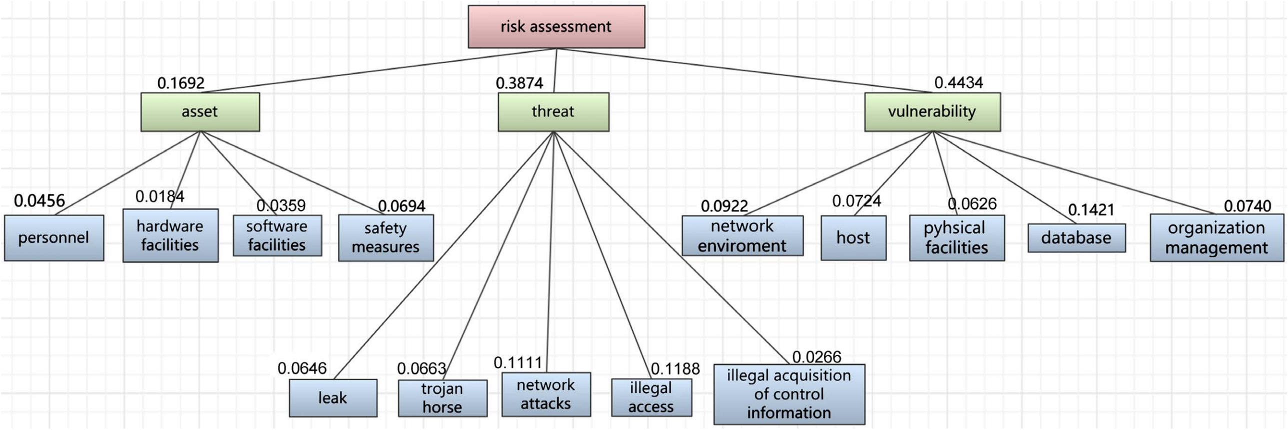


Figure 6. Risk assessment hierarchy.

of AHP, Yaahp [12], it can be used to make simple model construction and calculation of the system as a reference basis. **Figure 6** shows the evaluation indicators and corresponding weight values of the system. From the figure, it can be seen that the weight value of vulnerability accounts for the ratio is the highest, and attention should be strengthened in this regard.

To analyze the relationship between the indicators in more detail, a sensitivity analysis can be performed on the indicators. Through sensitivity analysis, it is possible to determine how the weight of each alternative will be affected when the weight of a certain element changes, to decide a higher level. To perform sensitivity analysis, first, complete the calculation of the ranking weight, and then obtain different sensitivity analysis tables based on different elements on the left structure tree generated by the hierarchical model structure. The curve in the table represents the change process of each index weight with the selected elements. It shows the sensitivity analysis of threat indicators during the assessment process. It can be seen that the weights of some indicators decrease with the increase of threats, and the weights of some indicators increase with the increase of threats, which can be more accurate Determine where safety protection measures need to be strengthened.

4.2. Consistency Check

According to the risk assessment process, we must first classify the system and construct a judgment matrix. The construction of the judgment matrix refers to the relevant data collected in the previous section and analyzed. Due to a large number of evaluation indicators in this article, there are a large number of discriminant matrices to be constructed, so this section only shows the judgment matrix related to threat indicators. The judgment matrix based on assets and vulnerability is also constructed in the same way as a pairwise comparison. Refer to the assignment of indicators. The influence of each index is quantified by the nine scaling index. The meaning of the nine scaling index is shown in **Table 1**, where $b_{ij} = b_i / b_j$, b_i and b_j respectively represent the evaluation size of the element *i* and elemrnt *j*.

Construct the judgment matrix according to Formula 1, and refer to **Table 1** to assign the judgment matrix. The judgment matrix for the second-level threat indicators is shown in **Table 2**. It is believed that the impact of human factors on the threat indicators is slightly greater than that of environmental factors. Therefore, the ratio of the importance of human factors to environmental factors is assigned a value of 3 in the judgment matrix.

Table 3 and **Table 4** show the different judgment matrices on human factors and environmental factors for the third-level indicators for illegally obtaining access rights, network attacks, leaks, Trojan horses, and illegally obtaining control information.

After constructing the judgment matrix, it is necessary to calculate its eigenvalues and whether it meets the consistency conditions, correct the unsatisfied judgment matrix to obtain a new matrix, and then calculate the index weights.

Table 1. Meanings of nine scaling index.

b_{ij}	Description of impact size and importance evaluation
1	Equally important
3	Slightly important
5	Obviously important
7	Very important
9	Extremely important
2, 4, 6, 8	Between the above description
reciprocal	Used to compare the importance of b_j and b_i

Table 2. Threat indicator judgment matrix *T*.

T	Human factors	Enviroment factors
Human factors	1	3
Enviroment factors	1/3	1

Table 3. Human factors judgment matrix *H*.

H	Illegal access	Network attacks	Leak	Trojan Horse	Illegal acquisition of control information
Illegal access	1	1	2	3	3
Network attacks	1	1	3	1/2	4
Leak	1/2	1/3	1	2	2
Trojan Horse	1/3	2	1/2	1	4
Illegal acquisition of control information	1/3	1/4	1/2	1/4	1

Table 4. Judgment Matrix of Environmental Factors *E*.

E	Illegal access	Network attacks	Leak	Trojan Horse	Illegal acquisition of control information
Illegal access	1	2	3	1/3	1/2
Network attacks	1/2	1	2	1/3	1/2
Leak	1/3	1/2	1	1	1/3
Trojan Horse	3	3	1	1	3
Illegal acquisition of control information	2	2	3	1/3	1

After calculating Tables 2-4, it can be seen that the judgment matrix of threat indicators meets the consistency condition; the maximum characteristic value of the human factor judgment matrix is 5.626, CR = 0.14 > 0.1, and it needs to be performed if the consistency condition is not met. Correction: The maximum

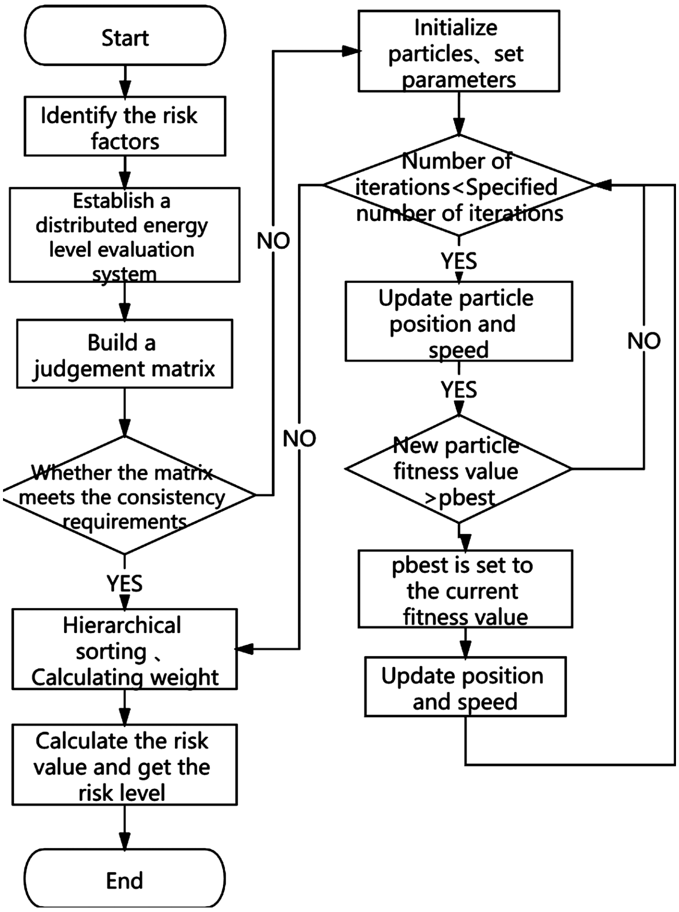

Start
Identify the risk factors
Establish a distributed energy level evaluation system
Build a judgement matrix
Whether the matrix meets the consistency requirements
YES
Hierarchical sorting、Calculating weight
Calculate the risk value and get the risk level
End
NO
Initialize particles、set parameters
Number of iterations<Specified number of iterations
YES
Update particle position and speed
YES
New particle fitness value >pbest
pbest is set to the current fitness value
Update position and speed
NO
NO

Figure 7. Consistency correction flow chart.

characteristic value of the environmental factor judgment matrix is 5.692, CR = 0.154 > 0.1, and the consistency condition needs to be corrected.

The Kalman particle swarm method is used to correct the matrix that does not meet the consistency. The specific correction process is shown in Figure 7. The particle swarm method can be used to find the optimal solution and modify the value of the judgment matrix. Since the larger the population, the better the convergence, but it will also affect the speed, so the maximum population is set to 20; to ensure the stability of the solution and reduce the calculation time, the number of iterations is set to 200; The inertia weight reflects the global optimization ability of the particle swarm, generally 0.5 - 1, this article sets it to $\omega = 0.7$; the value of the learning factor will affect the convergence of the population, and it is set to $c_1 = 1.5$, $c_2 = 1.6$ based on experience.

The parameter values of the revised judgment matrix can be shown in Figure 8, and it can be seen from the figure that the revised parameter values are significantly improved compared with the previous ones. In particular, there is an obvious gap between the 4th and 10th parameters. Therefore, the initial judgment matrix setting has a strong subjectivity problem, which leads to inconsistencies in the subsequent calculation process. After the particle swarm method and the improved particle swarm method optimize the parameter values, this problem is

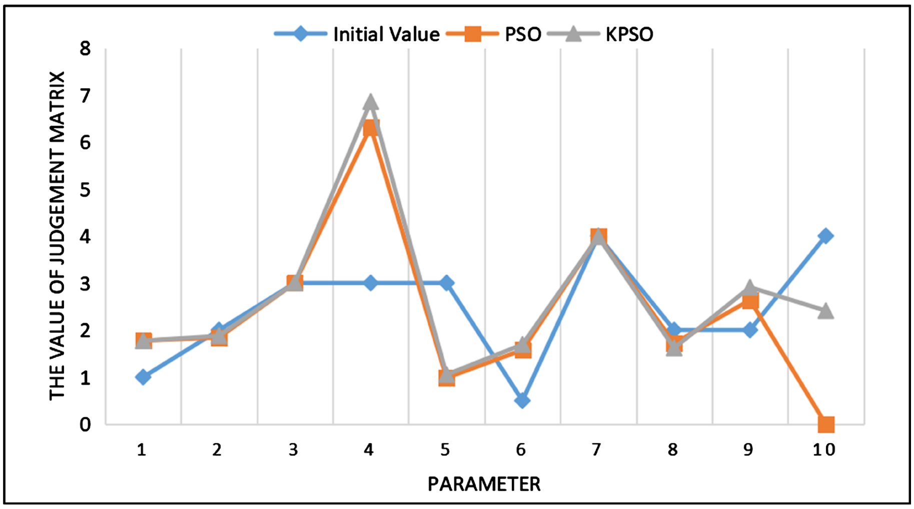


Figure 8. Revised result.

Table 5. Judgment matrix of environmental factors.

	CR	CI	Number of iterations
Initial value	0.14	0.157	
PSO	0.012	0.01344	100
KPSO	0.001 1	0.001232	80

effectively improved, so that the revised judgment matrix does not have the problem of failing the consistency check. Calculate whether the revised judgment matrix meets the consistency condition, and the results are shown in Table 5. The revised CR is all less than 0.1.

4.3. Calculate the Weight of the Evaluation Index

The evaluation indicators in this article are divided into three first-level indicators and seven second-level indicators. Through the establishment of the evaluation method and evaluation system in the previous sections, this section calculates the weight of each indicator relative to the target layer.

The index level for asset evaluation selects hardware facilities, software facilities, safety protection measures, and personnel; the criterion level is the three elements of confidentiality, integrity, and availability. First, the fuzzy analysis method is used to process the evaluation and scoring results of the experts, and the weight of each index relative to the asset is calculated. From Table 6, it can be seen that the usability value of the statistical assets is the highest, followed by completeness. Combining the weights of the three indicators, we can see that the asset value of security protection facilities and software facilities is higher.

The evaluation index layer for system threats selects five indicators of illegal access rights, network attacks, leaks, Trojan horses, and illegal access to control information; the criterion layer uses two indicators: environmental factors and

Table 6. Asset Index weight.

	Relative weight			Asset weight
	Confidentiality 0.11994	Integrity 0.2721	Availability 0.60796	
Hardware facilities	0.1087	0.26226	0.23008	0.22427
Software facilities	0.26625	0.45517	0.1993	0.27695
Safety protection measures	0.20835	0.14109	0.47391	0.35149
personnel	0.4167	0.14109	0.09671	0.14716

Table 7. Threat index weight.

	Relative weight		Threat weight
	Human factors 0.75019	Enviroment factors 0.24981	
Illegal access	0.22019	0.31325	0.24343
Network attacks	0.19168	0.11268	0.17194
Leak	0.29054	0.11268	0.2461
Trojan Horse	0.181	0.33818	0.22026
Illegal acquisition of control information	0.11659	0.12321	0.11824

human factors. The weight of each indicator can be shown in Table 7. It can be seen from the table that for distributed energy systems, the weight of human factors is higher than that of environmental factors, and the risk of illegal access rights and leaks is relatively high. Potential threats that are prone to occur, and protective measures in this area should be strengthened.

For the evaluation index layer of vulnerability, five evaluation indexes are selected: network environment, system host, physical facility, database and organization management; the criterion layer uses technical factors and management factors as evaluation indexes. The relative weight and vulnerability weight of each indicator can be shown in Table 8. It can be seen from the table that the weight of technical factors is higher than that of management factors. The weights of organizational management and network environment are higher than other indicators. The supervision of staff should be increased, relevant regulations should be revised, and network monitoring should be strengthened.

Synthesizing the weights of the indicators in Tables 5-7 can be used to obtain the total evaluation indicator weight, that is, the weight of each secondary indicator relative to the asset, threat, and vulnerability of the primary indicator, and the weight of the target layer weights.

4.4. Evaluation Result Analysis

The weight of each evaluation index calculated in the previous section can be obtained through the risk calculation formula, and it can be concluded that the

Table 8. Vulnerability index weight.

	Relative weight		Vulnerability weight
	Technical factors 0.8	Management factors 0.2	
Network environment	0.20412	0.18765	0.22962
Host	0.16844	0.11391	0.15753
Physical facility	0.14115	0.10629	0.13417
database	0.34641	0.22936	0.323
Organization Management	0.13987	0.36279	0.18445

information security risk level of the distributed energy system is between 3 - 4 levels, and security inspections should be carried out regularly to strengthen security protection measures.

This paper uses the fuzzy analytic hierarchy process to calculate the information security risk value of the small distributed energy system, and according to the security risk assignment table, it can be concluded that the security risk level is medium, which is in a relatively safe stage. However, it can be seen from the weight of each indicator that some indicators have higher risk values, and more attention should be paid to adopt targeted safety protection measures and adopt regular inspections.

For system assets, security protection measures and software facilities have a relatively high weight, which also shows that in the overall structure of the system, field equipment and various software facilities of the central control layer are mainly used to realize energy utilization and data transmission. And whether to install protective measures in the system is very important to maintain the safety and stability of the system. After weighing the threat and vulnerability indicators, it can be seen that there are many security problems in the system, including communication protocol vulnerabilities, inadequate protection measures, and database identity authentication issues. In the threat assessment, the security weight of illegal access and leaks is relatively high. In normal use, the access control of the system should be strengthened, and the identity authentication mechanism should be established. For common network attack characteristics, intrusion detection models can be established, early Find abnormalities and minimize damage. Because of the possible vulnerabilities in the system, there are some problems in the network environment and organization and management. The existence of these safety problems is a huge hidden danger to the long-term operation and operation of the system.

In response to the above possible problems, some security suggestions are put forward: The control access mechanism of the system should be strengthened, and multiple user authentication methods should be adopted for systems with higher security to prevent tampering and other behaviors that may reveal key information; establish targeted Intrusion detection model, the model should include the abnormal state when common various attacks occur, and the database of the intrusion detection model should be updated regularly; the on-site infrastructure should be sent to carry out regular inspections to check whether the controller of the equipment is normal To prevent accidents from being signaled and transmitted to the central controller in time; strengthen the safety protection awareness of internal staff, and write safety protection regulations and rules.

5. Conclusion

In this paper, the risk assessment of the distributed energy system is carried out based on the fuzzy analytic hierarchy process and a detailed evaluation index system is also established. Through the improved particle swarm optimization method, the unreasonable consistency of the judgment matrix of the analytic hierarchy method is investigated. Through the improved judgment matrix, the weight of each indicator has been corrected and obtained. And the improved particle swarm method has improved its iteration speed and accuracy. The final evaluation results show that possible problems can be effectively revealed, which provides a reference for the security protection of distributed energy stations.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] GB/T 20984-2007 (2007) Risk Assessment Specification for Information Security.

[2] GB/Z 24364-2009 (2009) Guidelines for Information Security Risk Management.

[3] Yu, Q. and Shen, Y.J. (2017) Research of Information Security Risk Prediction Based on Grey Theory and ANP. *Electronic and Automation Control Conference*, Xi'an, 107-113.

[4] Huang, X.P. and Xu, W. (2018) Method of Information Security Risk Assessment Based on Improved Fuzzy Theory of Evidence. *International Journal of Online Engineering*, **14**, 188-196. https://doi.org/10.3991/ijoe.v14i03.8422

[5] Zhang, L.J. and Wang, Q.X. (2010) A Network Security Evaluation Method Based on Fuzzy and RST. *International Conference on Education Technology and Computer*, Shanghai, Vol. 2, 40-44.

[6] Han, X., Guo, Y., Wang, H., *et al.* (2018) Study on the Risk Assessment of Power Operation Information Security Management Based on AHP. *Foreign Electronic Measurement Technology,* **37**, 32-37.

[7] Ren, Q., Pan, G., Bai, Y.Q., *et al.* (2018) Security Risk Assessment of Information System Based on FAHP and Attack Tree. *Application of Electronic Technique*, **44**, 113-117.

[8] Shang, W.L., Zhang, S.S., Wan, M., *et al.* (2014) Modbus/TCP Communication Anomaly Detection Algorithm Based on PSO-SVM. *ACTA Electronica Sinica,* **42**, 2315-2320.

[9] Dai, S.W., Wang, K.H. and Qian, J.X. (2015) Rapid Calibration Method for Accelerometer Based on AKPSO Algorithm. *Transducer and Microsystem Technologies*,

34, 69-72.

[10] Kennedy, J. and Eberhart, R.C. (1995) Particle Swarm Optimization. *Proceedings of IEEE International Conference on Neural Networks,* 1942-1948.

[11] Chai, J.W., Wang, S., Liang, H.H., *et al*. (2017) An AHP-Based Quantified Method of Information Security Risk Assessment Elements. *Journal of Chongqing University*, **40**, 44-53.

[12] Wang, H.G., Zhao, Y.S., Gao, F.J., *et al*. (2019) Factor Analysis and Reliability Evaluation of Power Supply Based on AHP. *Microcomputer Applications*, **2**, 102-106.