Information Security Risk Assessment of Hazardous Chemicals Emergency Command System Based on AHP-Fuzzy Comprehensive Evaluation Model

To cite this article: Jufeng Zhang et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 612 052004

View the article online for updates and enhancements.
Information Security Risk Assessment of Hazardous
Chemicals Emergency Command System Based on AHP-
Fuzzy Comprehensive Evaluation Model

Jufeng Zhang, Ke Gai*, Fengfeng Yang, Rili Yang and Siyang Wang
School of Energy Engineering, Longdong University, Qingyang, 745000, China

*Corresponding author e-mail: 365713625@qq.com

Abstract. Emergency command system is the hub of dealing with emergencies, which is of great significance to emergency rescue. In order to establish a more perfect emergency command system, considering the characteristics of strong subjectivity and large error in qualitative evaluation of information security system, based on AHP (Analytic Hierarchy Process) and Fuzzy (Fuzzy Analysis) evaluation method, this paper uses AHP-Fuzzy comprehensive evaluation model to quantitatively evaluate the information security of emergency command system of a hazardous chemical production enterprise in Qingyang, and calculates the risk. The validity of the discriminant model is verified.

1. Introduction
The emergency command system is a response mechanism system for the government and other public institutions to prevent, deal with, and manage the aftermath of emergencies in advance, so as to ensure the safety of public life and property, even to promote the harmonious and healthy development of society. However, with the rapid development of the Internet and information technology, information system security issues are increasingly serious, effective identification of system risks, and the development of corresponding preventive measures, has become an important part of information security.

Domestic and foreign scholars have done a lot of research work on information security risk assessment. Jiwnani, Zelkowitz [1] analyzed the weaknesses of Windows and Linux systems, and identified the causes, positions and influences. Hedbom [2] studied and analyzed the security features and weaknesses of Windows NT and Unix systems. Ritchey [3] used the network vulnerability model to detect the network attack graph. Jajodia [4] obtained a network topology vulnerability analysis tool based on the EDG (Exploit Dependency Graph) model, which played a positive role in the optimization of network security. Henning [5] built the visualization framework of system vulnerability, and analyzed comprehensively the weakness of system network. Wang lidong [6] quantified the weaknesses of Windows NT, Linux and Solaris systems.

In view of the importance of hazardous chemicals emergency command system in emergency rescue, in order to improve the accuracy of safety risk assessment, this paper carries out system information security assessment by combining hierarchical analysis and fuzzy evaluation.
2. AHP-Fuzzy Comprehensive Evaluation Model

2.1. AHP Evaluation Model
Risk is the damage of information system assets caused by system vulnerability, which is the product of information asset value and probability of events. Therefore, the system risk assessment must first determine the asset value, then analyze its threat and vulnerability, and finally get the system risk. By calculating the possibility of security incidents caused by vulnerability and assessing the extent of damage to assets caused by security incidents, the risk of the system is obtained.

\[ R = f(A, V, T) \]

Among them, \( R \) represents risk, \( A \) represents assets, \( V \) represents vulnerability, and \( T \) represents threat.

System risk is determined by the probability and the impact of its occurrence. In addition, the controllability of risk should be considered. The risk probability, risk impact and uncontrollability should be defined as the criterion layer [7]. The threat and vulnerability of the system should be defined as the scheme layer. Figure 1 is the structural model of an information system [8].

![Information System Architecture Model](image)

**Figure 1. Information System Architecture Model**

2.2. Asset Evaluation Model

(1) Asset value factor set \( B \) is composed of risk probability, risk impact and uncontrollability of asset information security, \( B = \{B_1, B_2, B_3\} \)

(2) Asset value evaluation set \( V \), \( V = \{1, 2, 3, 4, 5\} \), \( V \) is determined by the assignment table of three attributes of information security.

(3) Establishing a mapping from asset value factor set \( B \) to evaluation set \( V \) \( f: B \rightarrow f(V) \).

The factors from set \( B \) to set \( V \) exist in the evaluation matrix \( R \), that is: \( R = (r_{ij})_{3 \times 5} \)

Among them, \( r_{ij} \) refers to the subordination degree of asset value factor \( i \) to asset value index \( j \).

(4) Comprehensive evaluation
The weight coefficients of each element in asset factor set \( B \) are determined, the set of weight coefficients is \( \omega = \{\omega_1, \omega_2, \omega_3\} \), in which, \( \sum_{i=1}^{3} \omega_i = 1 \)

Normalization is implemented: \( B = \omega \times R \)

Formulas for calculating asset value are obtained:

\[ V_A = \text{int}\{B \times V^T\} \]  \( (1) \)

2.3. Threat Assessment
Information systems are threatened by the loss of confidentiality, integrity and availability of system assets due to attacks. The frequency and intensity of threats are directly related to the possibility and
loss of security incidents. Therefore, threat assessment assignment can be determined by the frequency and intensity of threats.

A single threat calculation formula for an asset is [9]:

\[ t = \text{int} \left( \frac{T_q + T_p}{2} \right), \quad T_q, T_p \in \{1, 2, 3, 4, 5\} \] (2)

Among them: \( t \)—asset threat; \( T_q \)—threat intensity; \( T_p \)—threat frequency.

Total threats to the assets of available information systems are obtained:

\[ T = \text{int}\left\{ \sum_{i=1}^{n} t_i / n + 0.5 \right\} \] (3)

2.4. Vulnerability Assessment

Information system vulnerability is closely related to the degree of asset damage, directly related to the size of information security risk value. Information system vulnerability can be assessed by identifying the vulnerability of assets and assigning values.

(1) Establishment of comparative judgment matrix

According to the established risk index system of the emergency command system for hazardous chemicals, several experts in the industry were invited to evaluate it by group decision-making method, and the judgment matrix was obtained by comparing the two indicators in the index system. The scale and description of the AHP method are shown in Table 1 [11]. The three attributes of the criterion layer are judged by two or two comparisons, and the comparative judgment matrix \( A-B \) is obtained.

\[
A - B = \begin{bmatrix}
    a_{11} & a_{12} & a_{13} \\
    a_{21} & a_{22} & a_{23} \\
    a_{31} & a_{32} & a_{33}
\end{bmatrix}, \quad \text{among them, } a_{ii} = 1, \quad a_{ij} = 1 / a_{ji} .
\]

| The value of \( a_{ij} \) | Meaning                              |
|--------------------------|-------------------------------------|
| 1                        | Element \( a_i \) is as important as element \( a_j \) |
| 3                        | Comparing elements \( a_i \) with \( a_j \), \( a_i \) is slightly important |
| 5                        | Comparing elements \( a_i \) with \( a_j \), \( a_i \) is important |
| 7                        | Comparing elements \( a_i \) with \( a_j \), \( a_i \) is more important |
| 9                        | Comparing elements \( a_i \) with \( a_j \), \( a_i \) is extremely important |
| 2, 4, 6, 8               | The median value between the two adjacent judgments |

The reciprocal of the above numbers Conversely, \( a_{ii} = 1 / a_{ij} \)

(2) Computation of eigenvectors of judgement matrices

The main methods of judgment matrix calculation are square root method and sum product method [10]. The eigenvalues of judgment matrix \( A-B \) and the weights of the elements in \( B \) are obtained, and then the eigenvectors are obtained by normalization.

The eigenvector of judgement matrix is computed: \( \omega^* = (\omega_1, \omega_2, ..., \omega_n) \), among them,

\[
\omega_i = \sqrt{\prod_{j=1}^{n} a_{ij}}, i = 1, 2,..., n
\]
Normalization is implemented: \( \omega = (\omega_1, \omega_2, \ldots, \omega_n)^T \), among them, \( \omega_j = \frac{\omega_j}{\sum_{i=1}^{n} \omega_i} \)

(3) Consistency test
In order to avoid the errors of evaluator in the evaluation process, the consistency test of the judgment matrix is carried out.

\[ I_c = \frac{\lambda_{\text{max}} - n}{n - 1} \]  \hspace{1cm} (4)

Consistency Ratio is:

\[ R_c = \frac{I_c}{I_R} \]  \hspace{1cm} (5)

The \( n \) is the number of first-order indicators, and \( I_R \) is the average random consistency index, as shown in Table 2 [11]. When \( R_c < 0.1 \), the judgment matrix is consistent; otherwise, when \( R_c > 0.1 \), the judgment matrix is inconsistent, the judgment matrix needs to be reconstructed until it has consistency.

| n  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|----|---|---|---|---|---|---|---|---|---|
| \( I_R \) | 0 | 0 | 0.58 | 0.90 | 1.12 | 1.24 | 1.32 | 1.41 | 1.45 |

(4) Identification of Information Assets Vulnerability
The eigenvector \( \omega_1 \) of the judgment matrix between criterion layer and the vulnerable point target layer, the eigenvector \( \omega_2 \) of the judgment matrix between the integrity and the vulnerable point, the eigenvector \( \omega_3 \) of the usability criterion and the vulnerable point judgment matrix are obtained by Hierarchical Single Sorting Method. The consistency test of the judgment matrices is carried out, the characteristic direction of the judgment matrix of the vulnerable point index layer to the asset attribute criterion layer is:

\[ \omega(2) = (\omega_1, \omega_2, \omega_3) \]  \hspace{1cm} (6)

According to \( \omega = \omega(1) \cdot \omega(2) \), the vulnerability score of asset A is obtained. According to Table 3 and vulnerability level, Vulnerability \( v_i \) is assigned V.

| Scope of judgement \( \omega \) | Vulnerability Assessment Level | Vulnerability assignment \( V \) |
|-----------------------------|-------------------------------|-------------------------------|
| \( \omega \leq 0.2 \)       | 1                             | 1                             |
| \( 0.2 < \omega \leq 0.4 \) | 2                             | 2                             |
| \( 0.4 < \omega \leq 0.6 \) | 3                             | 3                             |
| \( 0.6 < \omega \leq 0.8 \) | 4                             | 4                             |
| \( 0.8 < \omega \leq 1.0 \) | 5                             | 5                             |

2.5. Risk Analysis
According to the literature [9, 12], the AHP-Fuzzy comprehensive risk assessment model formula expressing the information security risk value of assets, threats and vulnerabilities is presented.

\[ R = R(A, V, T) \times (1 - EI) = R(L(T, V), F(\text{la}, V\alpha)) \times (1 - EI) \]

\[ = (1 - EI) \sqrt{\int \left[ \sum_{i=1}^{n} t_i / n + 0.5 \right] \cdot \bar{V} \cdot \text{int} \{ B \times V \} \cdot \bar{V}} \]  \hspace{1cm} (7)
Among them, \( R \)-risk value, \( A \)-asset, \( V \)-vulnerability, \( T \)-threat, the role value of la-security incidents on assets, the severity of \( V \)-vulnerability, the possibility of security incidents caused by the vulnerability of \( L \)-threat using assets, the loss of system assets caused by \( F \)-security incidents, and the effectiveness index of \( E \)-risk control measures.

3. Risk Safety Assessment Based on AHP-Fuzzy Comprehensive Judgment

Based on AHP-Fuzzy comprehensive evaluation mathematical model, the risk assessment of emergency command system of a hazardous chemical production enterprise in Qingyang was carried out.

(1) According to the asset evaluation model, the factor set of the database \( U = \{C, I, U\} \), and the value index set of the database \( V = \{1, 2, 3, 4, 5\} \) are made. Through interviews with system administrators and relevant experts [13], the evaluation set \( R \) is as follows:

\[
R = \begin{bmatrix}
0.1 & 0.05 & 0.1 & 0.2 & 0.4 \\
0 & 0.1 & 0.1 & 0.2 & 0.5 \\
0 & 0 & 0.1 & 0.6 \\
\end{bmatrix}
\]

If the weight \( v=(0.2,0.3,0.5) \) between confidentiality (C), integrity (I) and availability (A), then the asset value of the information system is:

\[
V_A = \text{int}\{v \times R \times V^T\} = \text{int}\{(0.2,0.3,0.5) \times \begin{bmatrix}
0.1 & 0.05 & 0.1 & 0.2 & 0.4 \\
0 & 0.1 & 0.1 & 0.2 & 0.5 \\
0 & 0 & 0.1 & 0.6 \\
\end{bmatrix} \times \begin{bmatrix}
1 \\
2 \\
3 \\
4 \\
5 \\
\end{bmatrix} \} = \text{int}\{3.66\} = 4
\]

(2) Based on the information security evaluation of the Emergency Command System website, some high-risk events are analyzed, such as operational errors, hardware and software failures, data leakage, malicious code, denial of service, etc. Threat formulas (2) and (3) are used, we obtain:

| Threat intensity | Operational errors | Software failure | Data leakage | Malicious code | Denial of service |
|------------------|--------------------|-----------------|--------------|----------------|------------------|
| Threat frequency | 4                  | 3               | 2            | 4              | 2                |
| Total threat value| \( \text{int}(2.8) \)=3 |                 |              |                |                  |

(3) Using Table 1 and expert's comparison judgment matrix \( A-B [6] \):

\[
A - B = \begin{bmatrix}
1 & 1/3 & 5 \\
3 & 1 & 7 \\
1/5 & 1/7 & 1 \\
\end{bmatrix}
\]

Calculate the judgment matrix \( A-B \), the eigenvector is \( \omega^*=(1.19,2.76,0.31) \), the normalized treatment is as follows:\( \omega=(0.28,0.65,0.07)^T \), the maximum eigenvalue is \( \lambda_{max}=3.045 \). When \( n=1, I_R=0.0225 \), the consistency index is \( IC=0.0388<0.1 \), which meets the consistency requirement. Eigenvector is \( \omega(1)=(0.28,0.65,0.07)^T \).

According to each expert's score, under the risk probability criterion, two pairs of contrast importance are formed, that is, the final comparison judgment matrix \( B-C^1, B-C^2, B-C^3 \).
The eigenvectors of the judgment matrix obtained by using MATLAB are as follows:

$$\omega(2) = (\omega_1, \omega_2, \omega_3)^T = \begin{bmatrix} 0.47 & 0.26 & 0.12 & 0.11 & 0.04 \\ 0.50 & 0.23 & 0.15 & 0.07 & 0.04 \\ 0.52 & 0.20 & 0.15 & 0.08 & 0.05 \end{bmatrix}$$

Therefore, the asset vulnerability score can be obtained:

$$\omega = \omega(1) \cdot \omega(2) = \begin{bmatrix} 0.28 & 0.65 & 0.07 \end{bmatrix} \begin{bmatrix} 0.47 & 0.26 & 0.12 & 0.11 & 0.04 \\ 0.50 & 0.23 & 0.15 & 0.07 & 0.04 \\ 0.52 & 0.20 & 0.15 & 0.08 & 0.05 \end{bmatrix} = \begin{bmatrix} 0.2005 & 0.2363 & 0.1416 & 0.0819 & 0.0407 \end{bmatrix}$$

The severity values of database vulnerability $v_1$, $v_2$, $v_3$, $v_4$ and $v_5$ are 0.2005, 0.2363, 0.1416, 0.0819, and 0.0407. According to table 3, the values of vulnerability $v_1$, $v_2$, $v_3$, $v_4$ and $v_5$ are 2, 2, 1, 1 and 1, respectively.

(4) The security measures adopted in the database of the emergency command information website are: professional training for system managers, setting up security passwords and setting up protection software, which to some extent weaken the vulnerability of $v_1$, $v_3$, $v_4$, and reference [6]. The validity index EI of risk control measures facing the database can be defined as 0.2.

(5) The risk value of information system under various vulnerabilities can be obtained by using the risk value calculation formula (7):

$$R_{v_i} = (1 - EI) \sqrt{\int \left( \sum_{i=1}^{n} t_i / n + 0.5 \right) \cdot V \cdot \sqrt{\int \{B \times V^T \} \cdot V}} = 0.8 \times \sqrt{48} = 2.63$$

4. Conclusion

A risk assessment model of information security based on fuzzy comprehensive evaluation and analytic hierarchy process is constructed. The risk assessment of information system is carried out by combining qualitative and quantitative methods. The website of a hazardous chemical emergency command system in Qingyang is verified by the new risk value calculation formula, and the validity and reliability of the results are obtained.
Acknowledgments
This work was financially supported by Gansu Safety Production Science and Technology Project (GAJ00004), China Association of Science and Technology (CAST) Project of Industry-University-Research Collaborative Innovation Consortium (ZLGCC201902) fund.

References
[1] K.Jiwnani, M.Zelkowitz.Maintaining Software with a Security Perspective. Proceedings of International Conference on Software Maintenance, Montréal, Canada, 2002: 194-203.
[2] H.Hedbom, S.Lindskog, S.Axelsson, et al. A Comparison of the Security of Windows NT and UNIX. Proceedings of Third Nordic Work shop on Secure IT Systems, Trondheim, Norway, 1998.
[3] R.Ritchey, P.Ammann.UsingModel Check ing to Analyze Network Vulnerabilities. Proceedings of IEEE Symposium on Security and Privacy, Oakland, California, 2000: 156-165.
[4] S.Jajodia, S. Noel, B.O Berry. Topological Analysis of Network Attack Vulnerability. ASIAN ACM Symposium on Information, Computer and Communications Security, 2005: 248-266.
[5] R.Henning, K.L. Fox The Network Vulnerability Tool (NVT)-A System Vulnerability Visualization Architecture. Proceedings of the 22nd National Information Systems Security Conference, Crystal City, VA, US, 1999: 97-111.
[6] Wang Lidong. Operating System Security Assessment and Audit Enhancement [D]. Harbin: Harbin University of Technology, 2002.
[7] T M Williams. The two-dimensionality of project ask [J]. International Journal of Project Management, 1996, 14 (3): 185-186.
[8] Dong-mei Zhao, Jing-hong Wang, Jing Wu, et al. Using Fuzzy Logic and Entropy Theory to Risk Assessment of the Information Security [A]. Proceedings of the 4th International Conference on Machine Learning and Cybernetics [C], Guangzhou, 18-21 August 2005, 2448-2453.
[9] WU Wen-gang, ZHANG Zhi-wen, WANG Qing-sheng. A Information Security Risk Assessment Model Based on AHP and Fuzzy Comprehensive Evaluation [J]. Journal of Chongqing University of Technology(Natural Science), 2017, 31 (7): 156-161.
[10] SHI Liang, ZHUANG Yi. Quantitative risk assessment model for network security. Computer Engineering and Applications, 2007, 43 (18): 146-149.
[11] Introduction to Security Risk Analysis and the COBRA Approach. http://www.Security policy.co.uk/riskanalysis.
[12] Li Pengyu. A Quantitative Method for Information Security Risk Assessment Based on Analytic Hierarchy Process [D]. Nanchang: Jiangxi University of Finance and Economics, 2012.