Received 20 August 2023, accepted 7 September 2023, date of publication 12 September 2023,
date of current version 20 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3314629

RESEARCH ARTICLE

Quantitative Evaluation Method for Industrial Control System Vulnerability Based on Improved Expert Elicitation and Fuzzy Set Method

WENLI SHANG[1], TIANYU GONG[2], JING HOU[3], JIAYUE LU[1], AND ZHONG CAO[1]
[1]School of Electronics and Communication Engineering, Guangzhou University, Guangzhou 510006, China
[2]China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China
[3]Information and Control Engineering Faculty, Shenyang Jianzhu University, Shenyang 110168, China

Corresponding authors: Tianyu Gong (gongtian_yu@163.com) and Zhong Cao (zhongc@gzhu.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2021YFB2012400, in part by the National Natural Science Foundation of China under Grant 62173101, in part by the Basic and Applied Basic Research Funding of Guangdong Province under Grant 2022A1515010865, in part by the Guangzhou Science and Technology Funding under Grant 202201020217, and in part by the Open Fund Project of Information Security Assessment Center of Civil Aviation University of China under Grant ISECCA-202201.

ABSTRACT For the problems of scientificity and reliability of vulnerability quantitative assessment method based on attack tree model, we propose an improved expert decision method based on attack tree model to improve the reliability of expert decision aggregation and solve the problem of insufficient evaluation data for the vulnerability quantitative evaluation method. Firstly, based on the expert decision aggregation method, the concept of deviation degree is proposed, and the maximum deviation degree method is innovatively proposed to screen fuzzy evaluations of experts. Then the deviation degree is taken as one of the influencing factors of fuzzy evaluations aggregation, and the expert fuzzy evaluations are aggregated to solve the problem of insufficient evaluation data. Finally, the improved expert decision aggregation method is combined with the vulnerability quantitative evaluation method based on the attack tree model to quantify the leaf nodes, security events, and attack sequence events. Using the ship industry control system as an illustration, we analyze and evaluate the feasibility and scientific validity of the proposed method. This analysis effectively enhances the reliability of the expert's fuzzy evaluation summary, solves the problem of insufficient evaluation data, and provides an important basis for the information security protection of the industrial control system.

INDEX TERMS Attack tree model, expert fuzzy evaluations, expert decision aggregation, vulnerability quantitative evaluation, ship industry control system.

I. INTRODUCTION

Industrial control system (ICS), as an important national infrastructure, has a direct impact on the development of the economy and trade. Under the influence of traditional IT networks, ICS is faced with a serious problem of information security [1]. Especially in recent years, under the background of the development of the Industrial Internet and 5G Communication Technology, the loss caused by the information security of ICS has attracted much more attention from governments all over the world.

Initially, due to the limitations of technological development, the traditional ICS was closed and independent. As a result, there is no unified management measure. The security problems of ICS mainly come from the local area network and the functions of components [2]. However, with the development of automation technology and IT network technology, information technology has been actively applied in modern ICS [3]. The interconnection of traditional ICS and IT networks will bring many serious security problems. Network attacks against ICS are growing at an alarming rate.

The associate editor coordinating the review of this manuscript and approving it for publication was Ton Duc Do.

Security incidents have caused huge losses to the government and related industries. The U.S. Department of Energy issued 21 measures to improve SCADA network security, which explicitly required system vendors to provide security functions for ICS devices [4]. Nevertheless, the Stuxnet [5] virus spread through U disk and other devices in the local area network in 2010 and attacked Iranian nuclear industrial facilities [6], [7], which caused ICS's security problems to be widely concerned. The security report from the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) stated that the number of attacks against ICS in 2016 still reached 290 and increased year by year [8]. ICS security problems not only lead to the paralysis of key infrastructure, but also may cause ecological problems, and even cause security accidents [9]. Security threat has gradually become the biggest challenge faced by industrial control systems, which needs to be studied and solved urgently [10].

The quantitative analysis of ICS vulnerabilities can effectively recognize the potential risks of the system to make corresponding defense measures, which has become the focus of current industry research. Since the control network structure, functions, and tasks of ICS are usually relatively fixed [11], [12], vulnerability analysis based on a graphical model is more suitable for ICS without frequent updates or modifications [12], [13]. Establishing the vulnerability correlation model of the evaluation system can better help security researchers analyze the vulnerability utilization principle and attack path, and find information security problems of the system in time. In addition, quantitative methods have been widely used in vulnerability assessment based on graph models, which can better allocate and effectively utilize information security resources [14], [15]. However, the modeling and quantification process relies heavily on the knowledge of security experts, which is usually incomplete or subjective [16]. This incompleteness and subjectivity will have a certain impact on the reliability of modeling and quantification. For large-scale complicated ICS, the problems of incompleteness and complexity of modeling can be solved by automatic modeling tools and optimization algorithms [17], [18]. Therefore, how to ensure the reliability and accuracy of quantitative evaluation is an open problem to be solved.

At present, the vulnerability quantification method based on the tree model has the problem of insufficient evaluation data and lack of processing of evaluation data, which makes the scientificity of the evaluation process and the reliability of the evaluation results affected by certain subjective factors [19], [20]. To solve the above problems and improve the reliability and scientificity of vulnerability quantitative assessment results based on the tree model, this paper provides an improved vulnerability quantitative assessment method based on the expert elicitation and fuzzy set (EEAFS) method. This method has been widely used in reliability analysis and achieved ideal results [21], [22]. However, this method can be further optimized in the process of expert decision-making and collection to improve the scientificity of expert decision aggregation. Based on the original, we first propose the concept of deviation degree and the maximum deviation degree method, which improves the reliability of the expert decision aggregation method. Through the combination of the improved expert decision aggregation method and the vulnerability quantitative evaluation method based on the attack tree model, the scientificity of the evaluation process and the reliability of the evaluation results are effectively improved.

The rest of this paper is organized as follows: The existing work and its problems are summarized in Section II. The improved expert fuzzy decision aggregation method is presented in Section III. Section IV introduces the quantitative evaluation method based on the attack tree model. A typical ICS as an evaluation case verifies the feasibility of the method proposed through the comparative analysis of different evaluation methods and evaluation results in Section V. Finally, the conclusion is in Section VI.

II. RELATED WORKS

A. FUZZY SET THEORY

Zadeh first proposed the theory of fuzzy sets in 1965 [23]. Traditional probability theory cannot effectively deal with ambiguous or uncertain events caused by subjective and objective factors. Fuzzy set theory can effectively deal with the influence of uncertainty or subjectivity, so it is widely used in various fields, including many engineering problems such as reliability analysis and risk assessment. Fuzzy set theory has been widely used in the evaluation method based on the fault tree model [24]. The fault tree is used for fault diagnosis [25] in systems, and the fuzzy fault tree had been used to analyze and evaluate the reliability of ship oil tanks [26], the chemical and petroleum industry [27], the coal mine industry [28], [29], and submarine pipelines [30]. A fuzzy probability Bayesian network (FPBN) approach was presented for dynamic risk assessment [31]. In the above methods, EEAFS are used to solve the reliability problem of the evaluation data. Fuzzy fault tree analysis mainly solves the reliability problem of evaluation data. However, the above methods lack expert evaluation and selection process, only consider the impact of the consistency and importance of experts, and lack of measurement of the overall deviation degree of evaluation, which makes fuzzy aggregation affected by the evaluation gap. To solve the above problems, this paper proposes an improved expert decision aggregation method based on EEAFS to improve the reliability of expert decision aggregation and provide reliable evaluation data for vulnerabilities quantitative evaluation based on the attack tree model.

In fuzzy set theory, fuzzy numbers can be used to express uncertain or fuzzy events in the process of analysis and evaluation of expert knowledge. Fuzzy numbers can be considered as a set of real numbers ranging from 0 to 1. Fuzzy numbers describe the relationship between the membership function $\mu_p(x)$ and probability P of uncertain events. Among

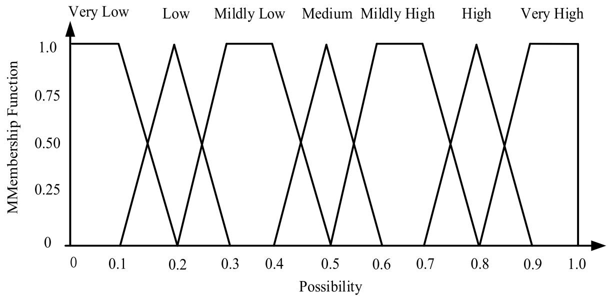


FIGURE 1. Membership function image.

all kinds of fuzzy numbers, triangular fuzzy numbers (TFN) and trapezoidal fuzzy numbers (TZFN) are usually used as evaluation languages. TFN is a vector (p_1, p_2, p_3), which can be represented by a set of four tuples $\tilde{\mathrm{P}}^{\alpha} = \{\alpha_{\mathrm{i}}, \mathrm{p}_1, \mathrm{p}_2, \mathrm{p}_3\}$ S, where α represents the confidence level of TFN. A typical membership function of TFN is shown in formula (1).

$$\mu_p(x) = \begin{cases} \dfrac{x-p_1}{p_2-p_1} & p_1 \le x \le p_2 \\ \dfrac{p_3-x}{p_3-p_2} & p_2 \le x \le p_3 \\ 0 & otherwise \end{cases} \quad (1)$$

Similarly, TZFN is a vector (p_1, p_2, p_3, p_4), which can be represented by a set of five tuples $\tilde{P}^{\alpha} = \{\alpha_i, p_1, p_2, p_3, p_4\}$. A typical membership function of TZFNs is shown in formula (2).

$$\mu_p(x) = \begin{cases} \dfrac{x-p_1}{p_2-p_1} & p_1 \le x \le p_2 \\ 1 & p_2 \le x \le p_3 \\ \dfrac{p_4-x}{p_4-p_3} & p_3 \le x \le p_4 \\ 0 & otherwise \end{cases} \quad (2)$$

In this paper, the multi-attribute utility theory is used to quantify the leaf nodes of the attack tree, so it is necessary for information security experts to evaluate the attributes of leaf nodes. Experienced evaluation experts usually have a rigorous scientific attitude in the evaluation process. They will use possibility language to describe the uncertainty of information security events, and use TFN and TZFN to quantify the possibility language [26], [27], [28], [29]. Figure 1 shows the membership function image corresponding to the fuzzy number. The language of fuzzy evaluation corresponding to the fuzzy number is shown in Table 1.

B. ATTACK TREE MODEL

The attack tree (AT) model [32] was first proposed by Professor Bruce Schneier of Carnegie Mellon University in 1999. It is intuitive, simple and easy to grasp, but it needs in-depth research and quantitative analysis, which is one of the commonly used graphical models in information security assessment. An AT graphically describes potential attack scenarios and systematically explains and classifies how attackers may attack systems or assets [33]. Security risk assessment in the industry has long appreciated attack trees as a means to solve cognitive scalability issues related to securing large systems [34].

TABLE 1. Fuzzy language.

Fuzzy Language	Abbreviations	Fuzzy Numbers
Very Low	VL	(0.0,0.0,0.1,0.2)
Low	L	(0.1,0.2,0.3)
Mildly Low	ML	(0.2,0.3,0.4,0.5)
Medium	M	(0.4,0.5,0.6)
Mildly High	MH	(0.5,0.6,0.7,0.8)
High	H	(0.7,0.8,0.9)
Very High	VH	(0.8,0.9,1.0,1.0)

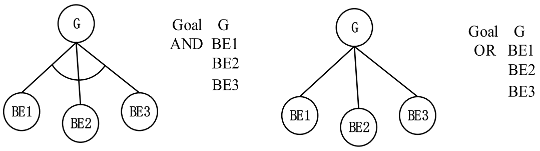


FIGURE 2. Attack tree model structure.

The AT (As shown in Figure 2) model is structured and hierarchically distributed, which is generated from bottom to top. Each leaf node of the AT is connected with its parent node through *AND* or *OR* nodes. Leaf nodes represent vulnerabilities in the systems or aggressive behavior. Attackers can AT root nodes only if they satisfy the conditions of leaf nodes and the corresponding logical conditions. The logical operator *AND* means that the root node event can only occur if all the leaf node conditions under the root node are satisfied at the same time, and the *OR* node means that the condition of any leaf node under the root node can be satisfied.

The quantitative evaluation method based on AT model has been widely used. In reference [35], the AT is used to analyze the security of the industrial physical network system. The paper describes the attributes of threats and vulnerabilities represented by leaf nodes in ATs. The threat and vulnerability vectors of attack paths are calculated using vector values. In reference [36], the AT model is used to construct the potential attack strategy of the attacker in the vehicle control network, and the attack defense tree is constructed to prevent the attack. In the above research, although the researchers used the AT model to analyze security problems accurately, the detailed risk quantification process is not given, and its effectiveness is not proven through comparative analysis. In reference [37], the risk analysis of abstract spatial information systems was carried out by using the improved AT model. The evaluation results can effectively solve the problem of security risk assessment of information systems based on space. In reference [38], the AT model was used to evaluate the threat and vulnerability of intelligent vehicle control systems. This method carries out a detailed analysis of the system threat and risk analysis and determines the risk assessment level by evaluating the risk. In reference [39], [40], [41], an AT model was used to model the vulnerability of rail transit, mobile intelligent terminals and power physical systems, and to evaluate the risks of the system. Although the detailed quantitative risk assessment method and process were given in the above research, the traditional probability assessment method does not solve the problem of uncertainty event quantification, and the probability assessment method will have a certain impact on the reliability of the assessment results. In reference [42], [43], [44], [45], [46], [47], the AT model was used to evaluate the vulnerability of airborne systems, ICS, and military business systems respectively, and the security attribute weight determination method was proposed. In order to solve the problem of uncertainty event quantification, a vulnerability quantitative evaluation method based on AT and fuzzy set theory is proposed [48]. However, to some extent, it only solves the problem of uncertainty event quantification and evaluation scientificity and cannot effectively solve the problem of insufficient evaluation data.

To solve the problem of reliability of expert decision aggregation and lack of evaluation data, an improved expert elicitation and fuzzy set (IEEEAFS) method for expert decision aggregation is proposed in this paper, which is combined with the vulnerability quantitative evaluation method based on AT model. In contrast to existing studies, this work has three main innovations.

(1) Set the maximum deviation degree when collecting fuzzy evaluations from experts, and if an expert's evaluation is lower than the maximum deviation degree, ask that expert to reevaluate.
(2) Introduce the deviation degree when calculating the comprehensive weights. Calculate the comprehensive weight factor through the relative consistency of experts, expert importance degree and deviation degree weight. Suppose the deviation of the fuzzy evaluation of an expert from the overall evaluation is larger. In that case, the reliability of the expert's evaluation is lower, and the weight it occupies is smaller.
(3) Combine with the quantitative vulnerability assessment method of AT to solve the problem of insufficient evaluation data in the quantitative evaluation method based on the AT model.

III. IMPROVEMENT OF EXPERT DECISION AGGREGATION METHOD BASED ON EEAFS

This section proposes a decision aggregation method based on IEEEAFS. In a traditional expert decision aggregation algorithm, there are the following problems: a) The method only collects and aggregates expert evaluation, lacking the screening process of expert evaluation. b) In the process of expert decision aggregation, only the relative consistency of experts and the influence of weight factors on fuzzy evaluation aggregation are considered, and the deviation degree is not measured. The above problems make the fuzzy aggregation results affected by those that deviated from the evaluation, which seriously affects the reliability of the evaluation results.

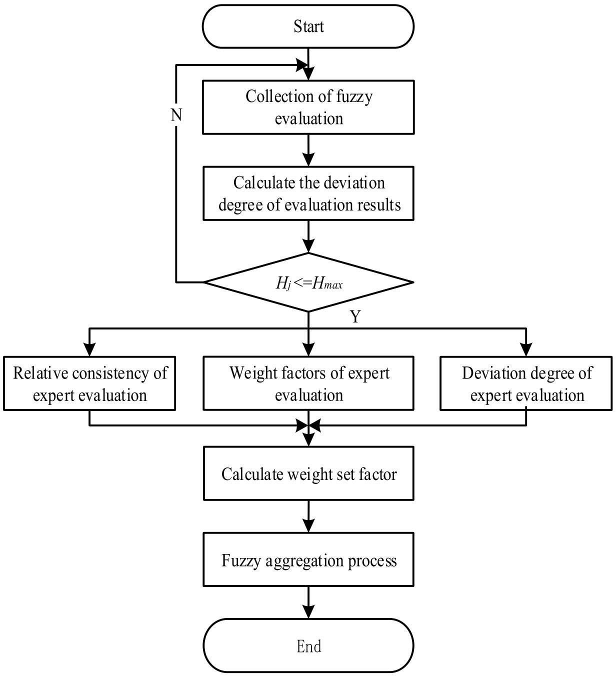

Start
Collection of fuzzy evaluation
N
Calculate the deviation degree of evaluation results
H_j<=H_{max}
Y
Relative consistency of expert evaluation
Weight factors of expert evaluation
Deviation degree of expert evaluation
Calculate weight set factor
Fuzzy aggregation process
End

FIGURE 3. Quantitative vulnerability assessment process.

TABLE 2. Fuzzy assessment standard.

Attack Cost		Attack Difficulty		Detected Possibility	
Level	F.L.	Level	F.L.	Level	F.L.
7	VL	7	VL	7	VL
6	L	6	L	6	L
5	ML	5	ML	5	ML
4	M	4	M	4	M
3	MH	3	MH	3	MH
2	H	2	H	2	H
1	VH	1	VH	1	VH

In order to solve the above problems, the concept of deviation degree is introduced on the basis of the traditional method, and the maximum deviation degree method is put forward innovatively. The deviation degree is used to screen expert evaluation, and it is regarded as one of the influencing factors of the aggregation factors of expert fuzzy evaluation to reduce the influence of the too large gap of expert evaluation on the evaluation results and improve the reliability of fuzzy aggregation. The flow chart of the expert decision aggregation method based on IEEAFS is shown in Figure 3.

Firstly, an expert evaluation group is set up to collect the fuzzy evaluation of each security attribute at the leaf node by each expert under the condition of anonymity among the expert members. Then, the deviation degree is used to screen the expert evaluation and judge whether the fuzzy evaluation of each expert meets the $H_j \leq H_{max}$ condition. If it meets the condition, the relative consistency of experts, the weight factor of experts and the weight proportion of deviation degree are calculated respectively to determine the aggregation weight factor. If it is not satisfied, the expert fuzzy evaluation deviation degree and the mean value of the evaluation set data are fed back to the experts who do not meet the requirements for re-evaluation. Finally, the expert evaluation is aggregated to get reliable evaluation results.

A. FUZZY ASSESSMENT COLLECTION

The possibility of security incidents is affected by many factors. The AT leaf nodes that represent system vulnerabilities or attack behaviors are affected by three factors: attack difficulty, attack cost, and detected possibility. In order to attack the target system, the attacker will carefully consider the influencing factors to make rational use of the vulnerability of the system and adopt effective attack methods, so as to improve the success rate of the invasion.

Although the attacker will pre-evaluate before attacking the system, there are still many uncertainties. Traditional probabilistic assessment techniques cannot effectively represent uncertain events, so it is necessary to use fuzzy numbers to deal with uncertain events. In addition, using a single expert knowledge for evaluation can affect the reliability of the evaluation results. To effectively reduce the impact of single expert knowledge on the reliability of the evaluation process and results, it is necessary to collect fuzzy evaluations made by multiple information security experts on the attributes of the AT leaf nodes. After evidence aggregation algorithm processing, more reliable evaluation results can be obtained. The assessment standard for leaf node attributes is shown in Table 2 (F.L. represents fuzzy language). The attack cost is proportional to the evaluation level and inversely proportional to the fuzzy language. The difficulty of attack and discovery are the same.

B. FUZZY EVALUATION SCREENING STAGE

According to the fuzzy evaluation of leaf nodes by experts collected, it is necessary to screen them to improve the reliability of fuzzy aggregation. The expert evaluation and selection process mainly includes the following aspects.

Step1: Calculation of deviation degree

The evaluation of different security attributes by experts will directly affect the reliability of the evaluation results. To improve the reliability of fuzzy aggregation, the distance between the whole fuzzy number evaluation data set is used to express the degree of deviation of expert evaluation, and the evaluation with excessive deviation is screened. The fuzzy evaluation data set of the ith security attribute A_i of each evaluation expert is $\left(\tilde{P}_{1i}, \tilde{P}_{2i}, \tilde{P}_{3i} \cdots \tilde{P}_{ni}\right)$.

The mean value $\bar{\tilde{\varphi}}_i$ of the evaluation data set is calculated, and its calculation formula is shown in (3).

$$\bar{\tilde{\varphi}}_i = \frac{1}{n}\sum\nolimits_{j=1}^{n} \tilde{P}_{ji} \tag{3}$$

Then, the deviation degree of each expert fuzzy evaluation from the whole evaluation set is determined. According to the fuzzy evaluation data set of the ith security attribute A_i and the mean value $\bar{\tilde{\varphi}}_i$ of the evaluation set, the deviation degree H_j between the expert evaluation data and the evaluation data as a whole can be calculated. If the fuzzy evaluation probability of the jth expert on the ith security Attribute is $\tilde{P}_{ji} = (a_1, a_2, a_3, a_4)$ and the mean value is $\bar{\tilde{\varphi}}_i = \left(\bar{b}_1, \bar{b}_2, \bar{b}_3, \bar{b}_4\right)$. The calculation formula of the deviation degree of the jth expert is shown in (4).

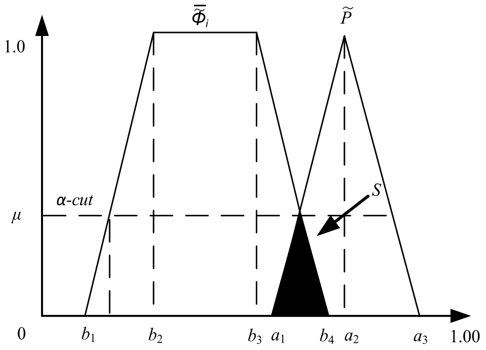


FIGURE 4. Scenario 1: Schematic diagram of deviation confirmation.

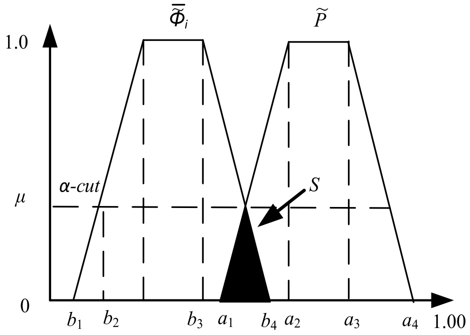


FIGURE 5. Scenario 2: Schematic diagram of deviation confirmation.

$$H_j = \sqrt{\frac{1}{4}\sum\nolimits_{j=1}^{m}\left|\left(\tilde{P}_{ji} - \bar{\tilde{\varphi}}_i\right)\right|} \tag{4}$$

where H_j indicates the deviation degree of expert fuzzy evaluation from the whole evaluation set. The value of H_j directly reflects the reliability of the expert evaluation. In order to improve the reliability of fuzzy evaluation aggregation, it is necessary to calculate the maximum deviation degree to achieve the screening of expert evaluation.

Step2: Calculation of maximum deviation degree

At present, there is not a specific and accurate method to determine H_{max} in the academic circle. Usually, the method of direct assignment is adopted according to the specific evaluation situation. This method has strong subjective factors and lacks certain scientificity. This paper creatively uses the image characteristics of the membership function in the traditional expert decision aggregation method and uses fuzzy evaluation mean and Euclidean distance to determine the upper limit of deviation degree.

In order to calculate the maximum deviation degree, the fuzzy evaluation data set with the ith security attribute is $\left(\tilde{P}_{1i}, \tilde{P}_{2i}, \tilde{P}_{3i} \cdots \tilde{P}_{ni}\right)$ and the fuzzy mean value is $\bar{\tilde{\varphi}}_i$, and the fuzzy evaluation is $\tilde{P}$. It should be noted that there are three situations for the composition of the evaluation data set. First, the fuzzy evaluation set consists of TFN and TZFN; second, the fuzzy evaluation set consists of TZFN; third, the evaluation data set consists of TFN.

When the mean value $\tilde{\bar{\varphi}}_i$ of fuzzy evaluation and the TFN $\tilde{P}$ is shown in Figure 4, i.e. $b_1 \leq a_1 \leq b_4$. In this paper, it is defined that when the shadow area of the membership function image $S = 0, a_1 = b_4$, the expert fuzzy evaluation $\tilde{P}$ has deviated from the edge of the overall evaluation level, and the maximum deviation degree $H_{TFN-max}$ can be calculated by Euclidean distance. When the mean value of fuzzy evaluation $\tilde{\bar{\varphi}}_i$ is opposite to the position of fuzzy number $\tilde{P}$, i.e. $b_1 \leq a_3 \leq b_4$, and $S = 0, a_3 = b_1$, the maximum value $H_{TFZN-max}$ of the maximum deviation degree can be calculated by Euclidean distance. We can obtain the value of $H_{TFN-max} = H_{TFN-max1}$, when $H_{TFN-max1} = H_{TFN-max2}$.

When the mean value $\tilde{\bar{\varphi}}_i$ of fuzzy evaluation and the TZFN $\tilde{P}$ have the position relationship as shown in the Figure 5, i.e. $b_1 \leq a_1 \leq b_4$, and $S = 0, a_1 = b_4$, the maximum deviation degree $H_{TZFN-max1}$ can be calculated the maximum deviation degree can be calculated by Euclidean distance. When the mean value of fuzzy evaluation $\tilde{\bar{\varphi}}_i$ is opposite to the position of fuzzy number $\tilde{P}$, i.e. $b_1 \leq a_4 \leq b_4$, and $S = 0, a_4 = b_1$, the maximum value $H_{TZFN-max2}$ of the maximum deviation degree can be calculated by Euclidean distance. We can obtain the value of $H_{TZFN-max} = H_{TZFN-max1}$, when $H_{TZFN-max1} = H_{TZFN-max2}$.

So, we can obtain $H_{max} = min \{H_{TFN-max}, H_{TZFN-max}\}$.

According to the above, the deviation degree of the *jth* expert's evaluation on the *ith* security attribute should meet the following conditions.

$$0 \leq H_j \leq H_{max} \tag{5}$$

When the fuzzy evaluation set is divided into the second and the third cases, the maximum deviation degree method is the same as the above principle.

In order to measure the deviation degree of the whole fuzzy evaluation set, the overall deviation degree H_J of the fuzzy evaluation defining the *ith* security attribute of the leaf node is shown in formula (6).

$$H_J = \frac{1}{n} \sum\nolimits_{j=1}^{n} H_j \leq H_{max} \tag{6}$$

Step3: Selection of expert evaluation If the deviation degree of any expert's fuzzy evaluation meets $H_J \leq H_{max}$, it shows that the data of the expert's fuzzy evaluation meets the reliability condition, and the expert's evaluation set can be further processed by fuzzy aggregation. If the deviation degree of any expert's fuzzy evaluation does not satisfy the deviation degree condition $H_J \leq H_{max}$, the fuzzy evaluation of that expert needs to be re-evaluated. We need to recalculate the deviation degree of the expert's evaluation until the deviation degree condition is been satisfied. Expert evaluation provides a reliable guarantee for the quantitative assessment of vulnerability.

C. FUZZY EVALUATION AGGREGATION STAGE

Step1: Computation of similarity degree In order to better reflect the similarity between different evaluations, the similarity matrix *SM* is used to represent the relationship between different evaluations. The similarity matrix *SM* is shown in formula (7).

$$SM = \begin{bmatrix} S_{11} & S_{12} & \cdots & S_{1n} \\ S_{21} & S_{22} & \cdots & S_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n1} & S_{n2} & \cdots & S_{nn} \end{bmatrix} \tag{7}$$

Each element S_{ij} in the similarity matrix *SM* refers to the similarity degree of different experts Ex_i and Ex_j for the same attribute evaluation, and it can also refer to the similarity between $\tilde{P}_i$ and $\tilde{P}_j$. The formula for calculating the similarity degree $S(\tilde{P}_i, \tilde{P}_j)$ is shown in (8).

$$S\left(\tilde{P}_i, \tilde{P}_j\right) = 1 - \frac{1}{4} \sum\nolimits_{i=1,j=1}^{4} \left|a_i - a_j\right| \tag{8}$$

In Formula (8), the similarity degree $(\tilde{P}_i, \tilde{P}_j)$. When the expert's opinion Ex_i is in complete agreement with Ex_j, $S(\tilde{P}_i, \tilde{P}_j) = 1$. In the process of calculating similarity measure, TFN should be transformed into TZFN for calculation.

Step2: Calculation of expert average agreement degree According to the similarity matrix *SM*, the average agreement degree $AA\,(Ex_i)$ of the *ith* experts is calculated, and the formula is shown in (9).

$$AA\,(Ex_i) = \frac{1}{n-1} \sum\nolimits_{i \neq j}^{n} S\left(\tilde{P}_i, \tilde{P}_j\right) \tag{9}$$

Step3: Calculation of relative agreement degree of experts According to the average agreement degree of experts, the relative agreement degree of experts $RA\,(Ex_i)$ is calculated. The calculation formula is shown in (10).

$$RA\,(Ex_i) = \frac{AA\,(Ex_i)}{\sum_{i=1}^{n} AA\,(Ex_i)} \tag{10}$$

Step4: Calculation of expert importance degree

Expert knowledge is influenced by many factors, such as education background, job position, work experience and age, which lead to different evaluation results. Considering the influence of these three factors on the evaluation process and results, it is necessary to determine the weight factor $W\,(Ex_i)$ of different experts in the evaluation. The calculation formula is shown in (11).

$$W\,(Ex_i) = \frac{w\,(Ex_i)}{\sum_{i=1}^{n} w\,(Ex_i)} \tag{11}$$

where $W\,(Ex_i)$ refer to the expert weight, $w\,(Ex_i)$ is the *ith* expert weight factor score. This paper determines the weight of experts using the method in [28]. Weighting scores for experts' significant degree are defined in Table 3.

Step5: Calculation of expert deviation degree weight

This paper defines that the greater the deviation of expert fuzzy evaluation from the overall evaluation, the lower the reliability of expert evaluation and the smaller the weight in

TABLE 3. Weighting scores of different experts.

Constitution	Classification	Score
Professional Position	professor	5
	Associate Professor	4
	Engineer	3
	Technical staff	2
	Lecturer	1
Work Experience (Year)	>20	4
	15-20	3
	10-15	2
	<10	1
Education Background	PHD	4
	Master	3
	Bachelor	2
	Junior college	1

the process of fuzzy set. The weight calculation formula of expert deviation is shown in equation (12).

$$W_h\left(Ex_i\right)=\frac{\frac{1}{H_j}}{\sum_{j=1}^{n}\frac{1}{H_j}}=\frac{1}{H_j\sum_{j=1}^{n}\frac{1}{H_j}} \tag{12}$$

Step6: Calculation of aggregation weighting factor

The aggregation weight factor of fuzzy evaluation can be obtained according to the calculated relative consistency of experts, expert importance degree and deviation degree weight. The calculation formula is shown in (13).

$$C\left(Ex_i\right)=\alpha W\left(Ex_i\right)+\beta W_h\left(Ex_i\right)+(1-\alpha-\beta)\,RA\left(Ex_i\right) \tag{13}$$

In Formula (13), $\beta, \alpha (0 \leq \beta \leq 1, 0 \leq \alpha \leq 1)$ is a relaxation factor, which is used to balance the relative agreement degree $RA\left(Ex_i\right)$, the expert importance degree $W\left(Ex_i\right)$ and the expert deviation degree $W_h\left(Ex_i\right)$. In this paper, we set $\alpha=\frac{1}{3}, \beta=\frac{1}{3}$.

Step7: Fuzzy aggregation

According to the aggregation weight factor of different experts, the final evaluation result $\tilde{P}_{A_i}$ is obtained by fuzzy aggregating the evaluation of multiple experts. The corresponding calculation formula is shown in (14).

$$\tilde{P}_{A_i}=\sum_{i=1}^{n}\left(C\left(Ex_i\right)\times\tilde{P}_i\right) \tag{14}$$

IV. FUZZY ATTACK TREE VULNERABILITY QUANTIFICATION ASSESSMENT METHOD

Through the collection, selection and aggregation of expert fuzzy evaluation, the reliability of fuzzy aggregation is improved. In addition, because expert evaluations are easy to collect, the problem of insufficient evaluation data is also solved, which can provide a reliable evaluation for vulnerability quantitative evaluation based on AT model. The detailed quantification analysis process is as follows.

Step1: Quantification of AT leaf nodes

In this paper, the expert inspired and fuzzy set theory expert decision aggregation method is combined with the vulnerability quantification evaluation method based on AT model to solve the problem of insufficient evaluation data and reliability of evaluation data. In order to ensure the integrity of this study, this paper refers to the AT leaf node quantification method in [41], [42], [43], and [44] and its specific quantification formula is shown in (15) and (16).

$$\tilde{P}_{A_i}^{\alpha}=\left[b_1+\alpha\left(b_2-b_1\right), b_4-\alpha\left(b_4-b_3\right)\right] \tag{15}$$

$$\tilde{P}_{SE_k}^{\alpha}=W_{cost}\times\tilde{P}_{SE_{cost\,k}}^{\alpha}+W_{diff}\times\tilde{P}_{SE_{diff\,k}}^{\alpha}+W_{det}\times\tilde{P}_{SE_{det\,k}}^{\alpha} \tag{16}$$

$\mathrm{W}_{\mathrm{cost}}, \mathrm{W}_{\mathrm{diff}}, \mathrm{W}_{\mathrm{det}}$ are the weight factors of attack cost, attack difficulty and detected possibility respectively. The weight factor satisfies $W_{cost}+W_{diff}+W_{detk}=1$. $\tilde{P}_{SE_k}^{\alpha}$ is the interval probability of the occurrence of leaf node events with $(1-\alpha)\,\%$ degree of confidence. $\tilde{P}_{SE_{diff\,k}}^{\alpha}$ is the interval probability of attack cost with $(1-\alpha)\,\%$ degree of confidence. $\tilde{P}_{SE_{det\,k}}^{\alpha}$ is the interval possibility of attack difficulty with $(1-\alpha)\,\%$ degree of confidence. $\tilde{P}_{SE_{det\,k}}^{\alpha}$ is the interval detected possibility with $(1-\alpha)\,\%$ degree of confidence. Formula (15) uses $\alpha-cut$ principle to determine the confidence interval of fuzzy evaluation and improve the reliability of evaluation. Where α $(\alpha\in[0,1])$ is confidence level. To compare with literature [48] under the same conditions, we take $\alpha=0.05$ in this paper.

In this paper, the weights of formula (16) are obtained after processing by analytic hierarchy process. The corresponding weights are $W_{cost}=0.37$, $W_{diff}=0.35$, $W_{det\,k}=0.28$.

Step2: Calculation of security events and attack sequences

According to the characteristics of AT structure, leaf nodes are connected with their parent nodes through logical nodes *AND* and *OR*. The interval probability formula for the occurrence of the parent node event E_n of leaf nodes connected by the logical *AND* is shown in (17).

$$\tilde{P}_{E}^{\alpha}=\prod_{i=1}^{k}\tilde{P}_{SE_k}^{\alpha} \tag{17}$$

The interval probability formula for the occurrence of the parent node event E_n of leaf nodes connected by the logical *OR* is shown in (18).

$$\tilde{P}_{E}^{\alpha}=1-\prod_{i=1}^{k}\left(1-\tilde{P}_{SE_k}^{\alpha}\right) \tag{18}$$

Attack sequence refers to a set of leaf nodes representing attack behavior or system vulnerabilities. In the attack subtree where the leaf node and its parent node are connected by the logical node AND, all the leaf node conditions need to be satisfied at the same time in order to complete an attack. The leaf node and its parent node are connected by logical node OR in the attack subtree, which satisfies the condition of any leaf node to complete an attack. The attack sequence $Sq_k=\left\{\tilde{P}_{Sq_1}, \tilde{P}_{Sq_2}, \cdots \tilde{P}_{Sq_n}\right\}$ is defined, and the interval probability of the attack sequence occurring is shown in formula (19).

$$\tilde{P}_{Sq_k}^{\alpha}=\tilde{P}_{SE_1}^{\alpha}\times\tilde{P}_{SE_2}^{\alpha}\times\cdots\times\tilde{P}_{SE_k}^{\alpha} \tag{19}$$

Step3: The process of defuzzification

In order to get the final precise probability value and facilitate the analysis and comparison of vulnerability risk, it is necessary to defuzzify the fuzzy numbers. In this paper, the area center method is used to realize the defuzzification, and its algorithm is shown in formula (20).

$$\begin{aligned} P_{defuzzication} &= \frac{\int x\mu_p(x)\,dx}{\int \mu_p(x)\,dx} \\ &= \frac{\int_{a_1}^{a_2} \frac{x-a_1}{a_2-a_1} xdx + \int_{a_2}^{a_3} xdx + \int_{a_3}^{a_4} \frac{a_4-x}{a_4-a_3} xdx}{\int_{a_1}^{a_2} \frac{x-a_1}{a_2-a_1} dx + \int_{a_2}^{a_3} dx + \int_{a_3}^{a_4} \frac{a_4-x}{a_4-a_3} dx} \\ &= \frac{(a_4+a_3)^2 - a_4a_3 - (a_2+a_1)^2 + a_2a_1}{3\,(a_4+a_3-a_2-a_1)} \end{aligned} \tag{20}$$

V. CASE ANALYSIS

A. FUZZY EVALUATION AGGREGATION STAGE

Based on the quantitative vulnerability assessment method proposed in this paper, the Ship Industry Control System (SICS) is used as a case to evaluate and analyze. Ships are an important means of transportation for maritime transport, which is of great significance to national economic development and foreign trade. Once a ship leaves the port and sails to the sea, it is like a city moving at sea. Its security is very important. With the development of automation technology and electronic information technology, modern SICS has eliminated the shortcomings of traditional SICS, such as closed, single control, low flexibility and lack of unified management, to realize integrated automation control of the whole ship. The architecture of the ship integrated automation control network is shown in Figure 6.

There are three main levels: management level, monitoring level and field equipment level. Field equipment level consists of field instruments, intelligent I/O units and controllers. Field equipment is distributed in different compartments due to their different functions. They are controlled by controllers. The controller transmits the collected control parameters to the monitoring layer through the gateway for processing and analysis, and stores them in the historical database. Management achieves unified management of the monitoring layer through the network connection. The management can exchange data with the remote-control center through the satellite public network. At the management level, the Electronic Chart and Information System (ECDIS) is responsible for the real-time state of ship navigation. It integrates the comprehensive information of the Global Positioning System (GPS) and the Automatic Identification System (AIS). GPS realizes ship navigation through remote satellites. AIS accomplishes navigation and communication between ships through ship-to-ship, AIS shore-based equipment and remote satellites.

Modern ship control network adopts intelligent, networked, digital, modular and integrated control to comprehensively monitor and manage the ship's resources, so that the equipment can run safely and reliably. Although this improves the ship's control efficiency and reduces the control difficulty, it also makes SICS network nodes numerous, branches complex and a huge data flow. Especially with access to the Internet, the vulnerability of SICS itself is exposed to the network. Some SICS lack cyber security protection and are very vulnerable to cyber-attack, which can even lead to the ship being hijacked. Therefore, the cyber security of ship control systems is especially important.

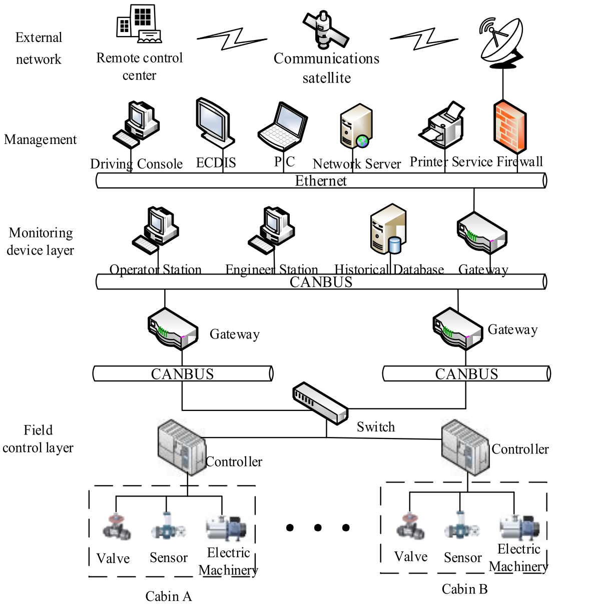


FIGURE 6. Ship control network architecture.

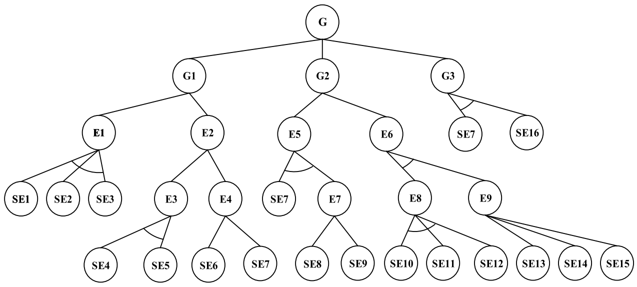


FIGURE 7. Attack tree model of ship control system.

The sophisticated network environment led attackers to tend to take multiple actions to achieve their goals [49]. The attacker will take advantage of the vulnerability of the system to invade, control and even destroy the ship control network in various ways. Attackers can use external public networks to intrude into the system. Firstly, attackers violently crack the encryption algorithm of information transmission and steal important data in the transmission process. Then, the important sensitive parameters in SICS are stolen through remote database injection. Finally, the remote execution of arbitrary code systems to control SICS management by exploiting the vulnerabilities in the mail. Attackers can attack GPS and AIS through private networks. By forging the GPS signal and tampering with the real-time data displayed in the GPS, the ship deviates from its original course. Taking advantage of the vulnerability of AIS software, the ship is forced to change course by sending wrong instructions to AIS. Attackers can also send a large amount of data to AIS, improve the fre-

TABLE 4. The meaning of leaf nodes.

Node Symbol	Node Meaning
G	Damage ship control system
G1	Attacks by external network
G2	Attacks control system controller
G3	Attacks through remote I/O units
E1	External public network intrusion
E2	Attacks through wireless and satellite private network
E3	Attacks Global Positioning System
E4	Attacks automatic identification system
E5	Attacks controller through network
E6	Physical ferry attack controller
E7	Get the link privileges of the controller
E8	Stuxnet virus self-installation
E9	Spread of Stuxnet virus
SE1	Mail server Vulnerability
SE2	Remote database injection
SE3	Violent decryption encryption algorithm
SE4	Tampering with or forging data
SE5	False GPS Signal Service
SE6	AIS Software Vulnerability
SE7	Denial of service attack
SE8	Crack the password to link with controller
SE9	Excessive access to the controller
SE10	Injection through U disk
SE11	Stealing digital certificate
SE12	Exploiting WinCC vulnerabilities
SE13	Windows shared file vulnerability
SE14	Printer offline vulnerability
SE15	Exploiting SMB protocol vulnerabilities
SE16	Physical Equipment Access Slave Station

TABLE 5. Results of different expert assessments.

Node symbol	Attack Cost			Attack Difficulty			Detected Possibility		
	Ex_1	Ex_2	Ex_3	Ex_1	Ex_2	Ex_3	Ex_1	Ex_2	Ex_3
SE1	MH	MH	ML	MH	M	ML	M	M	L
SE2	MH	M	ML	M	ML	M	MH	MH	ML
SE3	M	L	MH	MH	M	MH	H	ML	H
SE4	H	M	H	H	M	MH	M	ML	MH
SE5	MH	M	MH	H	MH	MH	M	M	MH
SE6	M	M	MH	MH	M	MH	MH	ML	M
SE7	ML	MH	L	M	MH	L	MH	H	ML
SE8	H	M	MH	MH	M	MH	M	MH	H
SE9	MH	H	M	H	MH	M	H	MH	ML
SE10	H	H	M	H	H	L	MH	M	ML
SE11	M	MH	MH	M	MH	M	MH	M	H
SE12	MH	L	M	MH	L	M	H	M	M
SE13	M	H	M	MH	H	M	ML	M	ML
SE14	M	MH	M	MH	MH	L	M	M	L
SE15	ML	MH	L	M	MH	L	MH	H	ML
SE16	M	H	ML	M	M	ML	MH	MH	L

TABLE 6. Deviation degree and maximum value of security attribute assessment set.

Node symbol	Attack Cost		Attack Difficulty		Detected Possibility	
	H_J	H_{max}	H_J	H_{max}	H_J	H_{max}
SE1	0.1333	0.3000	0.1117	0.2838	0.1333	0.2550
SE2	0.1005	0.2838	0.0703	0.2688	0.1333	0.3000
SE3	0.1687	0.2688	0.0703	0.2838	0.2012	0.2688
SE4	0.1333	0.2550	0.1117	0.2838	0.1117	0.2838
SE5	0.0703	0.2838	0.0703	0.2838	0.0703	0.2357
SE6	0.0703	0.2357	0.0703	0.2838	0.1117	0.2838
SE7	0.1687	0.2838	0.1687	0.2688	0.1687	0.2838
SE8	0.1117	0.2838	0.0703	0.2838	0.1687	0.2838
SE9	0.1117	0.2838	0.1117	0.2838	0.1687	0.2838
SE10	0.1333	0.2550	0.2667	0.3000	0.1117	0.2838
SE11	0.0703	0.2838	0.0703	0.2357	0.1203	0.2638
SE12	0.1697	0.2686	0.1687	0.2688	0.1321	0.2550
SE13	0.1333	0.3000	0.1117	0.2838	0.0878	0.2838
SE14	0.1117	0.2838	0.2012	0.2838	0.1333	0.2550
SE15	0.1687	0.2838	0.1687	0.2688	0.1687	0.2838
SE16	0.1687	0.2357	0.0703	0.2688	0.2012	0.2838

quency of data exchange, and seriously interfere with ship navigation.

The controller is an important target of attackers. The attacker can first crack the controller link password through an external device. Then, it establishes a link with the controller to obtain access rights beyond the authority. Finally, denial-of-service attacks are used to exploit the controller buffer overflow vulnerability, which affects the availability of the controller. Industrial viruses also pose a great threat to control systems. For example, the Stuxnet virus [5] is injected into the control system by physical ferry through a U disk. It uses the vulnerability of system software to complete the process of self-installation and diffusion to control and destroy the control system. In addition, an attacker can establish a connection with slave devices through external devices and use denial-of-service attacks to affect the availability of field devices to attack SICS.

Through the vulnerability analysis of the ship control system, the relationship between vulnerabilities is determined and the AT model is established. The AT model is shown in Figure 7, and the meaning of each node is shown in Table 4.

In order to complete the collection evaluation, three experts engaged in information security work are selected from a large number of candidate experts to form an evaluation team, and the evaluation of security attributes by each expert is collected. The collected results are shown in Table 5.

Due to the repeated collection, screening and feedback process of expert fuzzy evaluation, the cycle is relatively long and complex, which cannot be reflected in the paper in detail. The fuzzy evaluation results in Table 6 are obtained by several rounds or even multiple rounds of screening and re-evaluation and meet the deviation condition of fuzzy evaluation.

According to the deviation degree data in Table 6, the overall deviation degree of each leaf node's security attribute evaluation set meets the conditions. It can be explained that after the concept of deviation degree screens the expert evaluation, the credibility of the expert fuzzy evaluation can be improved so as to improve the reliability of the fuzzy aggregation.

Then the weight of relative consistency, weight factor and deviation degree of experts are calculated. The relative consistency of experts can be calculated by the formula (7), (8), (9), and (10). Table 7 shows the specific information of each evaluation expert and the weight index to the importance of the expert calculated by the formula (11). Using the formula (12) to determine the deviation degree of fuzzy evaluation of

TABLE 7. Assessment expert information form.

Expert	Professional Position	Work Experience (Year)	Education Background	Weight index
Ex1	Professor	>20	PHD	0.3940
Ex2	Associate Professor	15-20	PHD	0.3330
Ex3	Engineer	10-15	PHD	0.2730

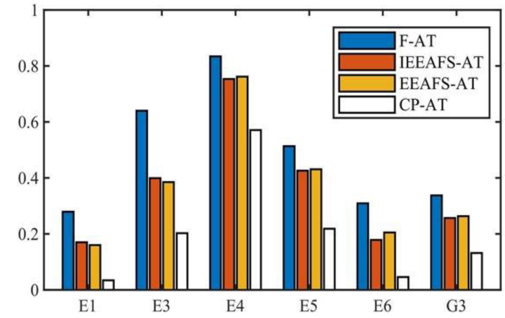


FIGURE 8. Probability distribution histogram of security event.

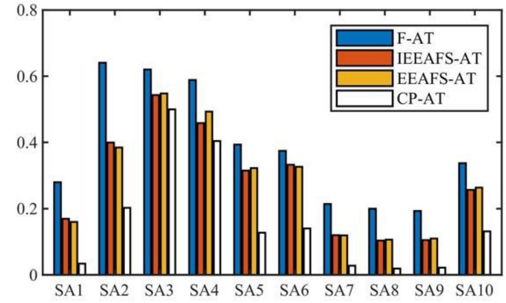


FIGURE 9. Probability distribution histogram of attack.

TABLE 8. The probability of security event.

Security Event	probability of security event
E1	0.1696
E3	0.3995
E4	0.7535
E5	0.4256
E6	0.1782
G3	0.2569

TABLE 9. The probability of attack sequences.

Attack Sequence S_{A_k}	Attack Sequence Set	probability of Attack Sequence
S_{A_1}	$\{SE_1$， SE_2， $SE_3\}$	0.1696
S_{A_2}	$\{SE_4$， $SE_5\}$	0.3995
S_{A_3}	$\{SE_6\}$	0.5433
S_{A_4}	$\{SE_7\}$	0.4587
S_{A_5}	$\{SE_7$， $SE_8\}$	0.3152
S_{A_6}	$\{SE_7$， $SE_9\}$	0.3327
S_{A_7}	$\{SE_{10}$， SE_{11}， SE_{12}， $SE_{13}\}$	0.1200
S_{A_8}	$\{SE_{10}$， SE_{11}， SE_{12}， $SE_{14}\}$	0.1034
S_{A_9}	$\{SE_{10}$， SE_{11}， SE_{12}， $SE_{15}\}$	0.1050
$S_{A_{10}}$	$\{SE_7$， $SE_{16}\}$	0.2569

TABLE 10. Comparison of advantages and disadvantages of EEAFS and IEEAFS.

Aggregation Method	EEAFS-AT[26-28]	IEEAFS-AT
Collection of evaluation	√	√
Selection of evaluation	×	√
Determination of deviation degree	×	√
Deviation degree	×	√
Relative consistency	√	√
Expert weight factor	√	√

TABLE 11. Comparison of advantages and disadvantages of various vulnerability quantitative assessment methods.

Assessment method	IEEAFS-AT	F-AT in [48]	CP-AT in [41-44]
Quantification of uncertain events	√	√	×
Scientificity of evaluation criteria	√	√	×
Whether the evaluation data is sufficient	√	×	×
Processing of evaluation data	√	×	×
Information lost in the evaluation process	×	×	√

experts from the overall evaluation. Finally, reliable evaluation data can be obtained by fuzzy aggregation.

The method of Section III-C is used to analyze the AT model. Firstly, leaf nodes are quantified, and then the probability of the security event and attack sequence event is calculated. Finally, the evaluation results are fuzzed to obtain accurate vulnerability risk values. Through the analysis of the AT model, six kinds of security events that can directly threaten the SICS are identified. From the perspective of the attacker, 10 attack sequences that can directly threaten the ship control network are determined. The probabilities of security events and attack sequence events obtained by calculation are shown in Table 8 and Table 9, respectively.

Because the security attributes of ''Attack Cost'', ''Attack Difficulty'' and ''Detected Possibility'' are difficult to be measured by objective data, the evaluation method based on the AT model suffers from the problem of insufficient evaluation data. In this paper, the expert decision aggregation methods of EEAFS and IEEAFS are combined with the quantitative evaluation method based on the AT model to solve the problem of insufficient evaluation data in the current evaluation method based on the AT model. At the same time, the feasibility and scientificity of the proposed method are verified by comparing several quantitative evaluation methods based on AT model. The probability distribution histogram of quantitative evaluation results is shown in Figure 8 and Figure 9, respectively.

The advantages and disadvantages of EEAFS and IEEAFS methods are shown in Table 10 and the advantages and disadvantages of various vulnerability quantitative assessment methods based on AT model are shown in Table 11.

B. FUZZY EVALUATION AGGREGATION STAGE

According to Figure 6, Figure 7 and Table 11, the methods EEFAF and IEEAFS are analyzed as follows. The method of EEFAS in the fuzzy aggregation process only collects and aggregates the fuzzy evaluation of experts, but lacks the screening process of fuzzy evaluation. In the process of fuzzy aggregation, only the relative consistency of experts and the weight factor of experts are considered. The lack of measurement of the degree of expert deviation will make the fuzzy aggregation results affected by the evaluation of excessive deviation and seriously affect the reliability of the evaluation results.

Based on the traditional method, this paper introduces the concept of deviation degree and puts forward a new maximum deviation degree method. To reduce the impact of the expert evaluation gap on the evaluation results and improve the reliability of fuzzy aggregation, the degree of deviation is selected as one of the influencing factors.

For Figure 8 and Figure 9, the main reason for the small difference between the two methods is that the evaluation data sets processed by the expert decision aggregation method after the improvement are from Table 6. The evaluation data in Table 6 are the evaluation results obtained after the collection, screening and reevaluation of expert evaluation. In EEAFS, there is no process of selecting, feedback and reevaluation of expert fuzzy evaluation. When the fuzzy evaluation of the same security attribute made by various experts is too different, the evaluation results of security events and attack sequences will greatly deviate from the evaluation results of IEEAFS, and even the vulnerability risk ranking will be different, which will seriously affect the reliability of the evaluation results.

Through the above analysis, the following conclusions are drawn: the improved expert decision aggregator proposed in this paper improves the scientificity of the expert decision aggregation process and the reliability of aggregation results.

According to Figure 8, Figure 9 and Table 11, a variety of vulnerability quantitative assessment methods based on AT model are analyzed as follows.

The vulnerability quantitative evaluation method in literature [41], [42], [43], [44] is based on the classical probability theory (CP-AT). There are two problems in the evaluation method of classical probability theory. (1) Classical probability theory can't solve the problem of quantifying uncertain events, which leads to information loss in the evaluation process. (2) Traditional methods lack the process of collecting, screening and aggregating expert evaluation data, which leads to the evaluation results being influenced by human subjective factors. The above causes directly lead to the probability of security events and attack sequence events, which deviates greatly from the method proposed in this paper.

The vulnerability quantitative evaluation method in literature [48] is based on fuzzy theory and attack tree (F-AT). Although the method solves the problem of uncertainty event quantification and scientific evaluation criteria, and avoids the problem of information loss in the evaluation process, the method still fails to solve the problem of reliability of evaluation data. The reliability of expert evaluation data is the main reason for the high evaluation results.

Through the above analysis, it is proved that the vulnerability quantitative assessment method proposed in this paper is feasible and can effectively improve the scientificity of the assessment process and the reliability of the assessment results.

According to Figure 8, the order of possibility of security event E_n occurrence is $E4 > E5 > E3 > G3 > E6 > E1$. From Figure 9, the order of possibility of attack sequence occurrence is $S_{A_3} > S_{A_4} > S_{A_2} > S_{A_6} > S_{A_5} > S_{A_{10}} > S_{A_1} > S_{A_7} > S_{A_8} > S_{A_9}$.

It can be seen from the above results that among ship control systems, the communication system is the most vulnerable target to network security threats. Attackers force the ship to change course or even hijack the ship by attacking the AIS or GPS, which poses a great threat to the safety of the ship. Attackers can also break into the communication network, steal transmission data, ship control parameters, and even deeply penetrate the ship's internal network. The controller is the key equipment in charge of network control and equipment operation inside the ship. Through the network to achieve the illegal intrusion of the controller, the attacker obtains the control authority of the ship control system, affects its availability, and even destroys and paralyzes the SICS. Injecting worms into the control network via external mobile devices can also have serious consequences for SICS. This virus is less likely to occur because of its difficulty in design, high specificity and poor concealment of the injection process. Attacks on remote I/O units mainly come from inside the ship. Attackers establish connections with remote distributed I/O systems through external physical devices and use denial of service attacks to affect the availability of I/O devices.

The results of a vulnerability quantitative assessment can effectively reflect the risks of the target system. However, there is no necessary relationship between the level of risk and the occurrence of events. Although the feasibility of some safety incidents is low, once they happen, they will lead to serious adverse consequences. Therefore, any risk should be attended to and security measures should be taken accordingly.

VI. CONCLUSION

In this paper, an IEEAFS-based expert decision aggregation method is proposed, which is combined with the vulnerability quantitative evaluation method based on AT model. This method can improve the reliability of the expert decision aggregation method, and solve the problem of insufficient evaluation data of existing vulnerability assessment methods based on AT model. The feasibility and scientificity of the proposed method are proved by comparing the evaluation results and analyzing the advantages and disadvantages of various methods. Through the analysis of the evaluation case results, the system's existing security risks are determined, which can provide an important basis for the information security protection of the industrial control system.

The industrial control system is a complex and huge control network. With the continuous development of the Internet, the complexity of industrial control systems is increasing, and its vulnerability is constantly exposed on the Internet. The complex network makes the hierarchical structure of AT model more complex, which leads to a serious model explosion and seriously affects the reliability of quantitative evaluation of information security. Although this paper improves the reliability of fuzzy aggregation to a certain extent and solves the problem of insufficient evaluation data, it is based on expert knowledge and traditional probability theory, so the evaluation process will be affected by human subjective factors. The future work will focus on how to get real data through semi-physical simulation [50] to further improve the reliability of the assessment results. The obtained assessment results are also used as a basis for intelligent deployment of the system [51].

REFERENCES

[1] E. G. Popkova, "Preconditions of formation and development of Industry 4.0 in the conditions of knowledge economy," *Industry 4.0: Industrial Revolution of the 21st Century*. Cham, Switzerland: Springer, 2019.

[2] S. Ponomarev and T. Atkison, "Industrial control system network intrusion detection by telemetry analysis," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 2, pp. 252–260, Mar. 2016.

[3] W. Knowles, D. Prince, D. Hutchison, J. F. Disso, and K. A. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Protection*, vol. 9, pp. 52–80, Jun. 2015.

[4] *21 Steps to Improve Cyber Security of SCADA Networks*, U.S. Department of Energy, Washington, DC, USA, 2005.

[5] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[6] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016.

[7] Z. Masood, R. Samar, and M. A. Z. Raja, "Design of a mathematical model for the Stuxnet virus in a network of critical control infrastructure," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101565.

[8] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). (2018). *Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-in-Depth Strategies November*. [Online]. Available: https://icscert.uscert.gov/sites/default/files/recommendedpractices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[9] E. N. Yılmaz and S. Gönen, "Attack detection/prevention system against cyber attack in industrial control systems," *Comput. Secur.*, vol. 77, pp. 94–105, Aug. 2018.

[10] X. Fan, K. Fan, Y. Wang, and R. Zhou, "Overview of cyber-security of industrial control system," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Aug. 2015, pp. 1–7.

[11] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proc. 3rd USENIX Workshop Hot Topics Secur.*, San Jose, CA, USA, Jul. 2008, p. 1158.

[12] M. R. Asghar, Q. Hu, and S. Zeadally, "Cybersecurity in industrial control systems: Issues, technologies, and challenges," *Comput. Netw.*, vol. 165, Dec. 2019, Art. no. 106946.

[13] N. Khakzad and G. Reniers, "Using graph theory to analyze the vulnerability of process plants in the context of cascading effects," *Rel. Eng. Syst. Saf.*, vol. 143, pp. 63–73, Nov. 2015.

[14] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, "Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems," *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 46, no. 10, pp. 1429–1444, Oct. 2016.

[15] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 24–45, Feb. 2015.

[16] Y. Qin, Y. Peng, K. Huang, C. Zhou, and Y.-C. Tian, "Association analysis-based cybersecurity risk assessment for industrial control systems," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1423–1432, Mar. 2021.

[17] J. Xu, E. Huang, L. Hsieh, L. H. Lee, Q.-S. Jia, and C.-H. Chen, "Simulation optimization in the era of Industrial 4.0 and the Industrial Internet," *J. Simul.*, vol. 10, no. 4, pp. 310–320, Nov. 2016.

[18] G.-Q. Zeng, J. Chen, Y.-X. Dai, L.-M. Li, C.-W. Zheng, and M.-R. Chen, "Design of fractional order PID controller for automatic regulator voltage system based on multi-objective extremal optimization," *Neurocomputing*, vol. 160, pp. 173–184, Jul. 2015.

[19] A. P. Henriques de Gusmão, M. M. Silva, T. Poleto, L. C. E. Silva, and A. P. C. S. Costa, "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory," *Int. J. Inf. Manage.*, vol. 43, pp. 248–260, Dec. 2018.

[20] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2016.

[21] E. Pourjavad and A. Shahin, "The application of Mamdani fuzzy inference system in evaluating green supply chain management performance," *Int. J. Fuzzy Syst.*, vol. 20, no. 3, pp. 901–912, Mar. 2018.

[22] Z. Hao, Z. Xu, H. Zhao, and Z. Su, "Probabilistic dual hesitant fuzzy set and its application in risk evaluation," *Knowl.-Based Syst.*, vol. 127, pp. 16–28, Jul. 2017.

[23] L. A. Zadeh, "Review of a mathematical theory of evidence," *AI Mag.*, vol. 5, no. 3, pp. 235–247, 1984.

[24] K. You, G. Qiu, and Y. Gu, "Rolling bearing fault diagnosis using hybrid neural network with principal component analysis," *Sensors*, vol. 22, no. 22, p. 8906, Nov. 2022.

[25] K. You, G. Qiu, and Y. Gu, "An efficient lightweight neural network using BiLSTM-SCN-CBAM with PCA-ICEEMDAN for diagnosing rolling bearing faults," *Meas. Sci. Technol.*, vol. 34, no. 9, Sep. 2023, Art. no. 094001.

[26] B. Ünver, S. Gürgen, B. Sahin, and İ. Altın, "Crankcase explosion for two-stroke marine diesel engine by using fault tree analysis method in fuzzy environment," *Eng. Failure Anal.*, vol. 97, pp. 288–299, Mar. 2019.

[27] M. Mohsendokht, "Risk assessment of uranium hexafluoride release from a uranium conversion facility by using a fuzzy approach," *J. Loss Prevention Process Industries*, vol. 45, pp. 217–228, Jan. 2017.

[28] S. Shi, B. Jiang, and X. Meng, "Assessment of gas and dust explosion in coal mines by means of fuzzy fault tree analysis," *Int. J. Mining Sci. Technol.*, vol. 28, no. 6, pp. 991–998, 2018.

[29] L. Giraud and B. Galy, "Fault tree analysis and risk mitigation strategies for mine hoists," *Saf. Sci.*, vol. 110, pp. 222–234, Dec. 2018.

[30] Y. Jianxing, C. Haicheng, Y. Yang, and Y. Zhenglong, "A weakest t-norm based fuzzy fault tree approach for leakage risk assessment of submarine pipeline," *J. Loss Prevention Process Industries*, vol. 62, Nov. 2019, Art. no. 103968.

[31] Q. Zhang, C. Zhou, Y.-C. Tian, N. Xiong, Y. Qin, and B. Hu, "A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2497–2506, Jun. 2018.

[32] B. Schneier, "Attack trees: Modeling security threats," *Dr. Dobbs J.*, vol. 12, no. 24, pp. 21–29, 1999.

[33] A. Arghavani, M. Arghavani, M. Ahmadi, and P. Crane, "Attacker-manager game tree (AMGT): A new framework for visualizing and analysing the interactions between attacker and network security manager," *Comput. Netw.*, vol. 133, pp. 42–58, Mar. 2018.

[34] O. Gadyatskaya and R. Trujillo-Rasua, "New directions in attack tree research: Catching up with industrial needs," in *Proc. Int. Workshop Graph. Models Secur.*, 2018, vol. 107, no. 44, pp. 115–126.

[35] F. Xie, T. Lu, X. Guo, J. Liu, Y. Peng, and Y. Gao, "Security analysis on cyber-physical system using attack tree," in *Proc. 9th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2013, pp. 429–432.

[36] M. Houmer, M. L. Hasnaoui, and A. Elfergougui, "Security analysis of vehicular ad-hoc networks based on attack tree," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Jun. 2018, pp. 21–26.

[37] W. Lv and W. Li, "Space based information system security risk evaluation based on improved attack trees," in *Proc. 3rd Int. Conf. Multimedia Inf. Netw. Secur., IEEE Comput. Soc.*, Nov. 2011, pp. 480–483.

[38] H.-K. Kong, M. K. Hong, and T.-S. Kim, "Security risk assessment framework for smart car using the attack tree analysis," *J. Ambient Intell. Humanized Comput.*, vol. 2, no. 3, pp. 1–21, 2017.

[39] H. Dong, H. Wang, and T. Tang, "An attack tree-based approach for vulnerability assessment of communication-based train control systems," in *Proc. Chin. Autom. Congr. (CAC)*, Oct. 2017, pp. 6407–6412.

[40] F. Wei and M. Zhang, "A risk assessment scheme of intellignet terminal based on attack tree," in *Proc. 4th Int. Conf. Cloud Comput. Intell. Syst. (CCIS)*, Aug. 2016, pp. 67–71.

[41] Y. Ru, Y. Wang, J. Li, J. Liu, G. Yang, K. Yuan, and K. Liu, "Risk assessment of cyber attacks in ECPS based on attack tree and AHP," in *Proc. 12th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Aug. 2016, pp. 465–470.

[42] H. Huang, S. Xiao, and H. Liang, "Safety vulnerability assessment of SCADA system based on AHP and attack and defense tree," *Control Eng.*, vol. 25, no. 6, pp. 1091–1097, 2018.

[43] L. He, Z. Chen, and X. Long, "An improved attack tree model based on AHP," *Comput. Appl. Res.*, vol. 33, no. 12, pp. 3755–3758, 2016.

[44] Z. Lu, W. Qi, and Z. Gu, "Attack tree model based on fuzzy analytic hierarchy process," *Comput. Eng. Des.*, vol. 39, no. 6, pp. 1501–1505, 2018.

[45] K. Kaynar and F. Sivrikaya, "Distributed attack graph generation," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 5, pp. 519–532, Sep. 2016.

[46] A. T. Al Ghazo, M. Ibrahim, H. Ren, and R. Kumar, "A2G2V: Automatic attack graph generation and visualization and its applications to computer and SCADA networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 10, pp. 3488–3498, Oct. 2020.

[47] M. Wan, W. Shang, and P. Zeng, "Double behavior characteristics for one-class classification anomaly detection in networked control systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 3011–3023, Dec. 2017.

[48] W. Shang, T. Gong, C. Chen, J. Hou, and P. Zeng, "Information security risk assessment method for ship control system based on fuzzy sets and attack trees," *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Mar. 2019.

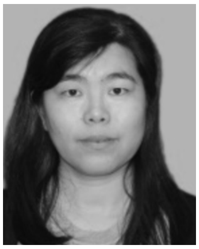
[49] F. Dai, Y. Hu, K. Zheng, and B. Wu, "Exploring risk flow attack graph for security risk assessment," *IET Inf. Secur.*, vol. 9, no. 6, pp. 344–353, Nov. 2015.

[50] K. You and H. Liu, "Research on optimization of control parameters of gravity shaking table," *Sci. Rep.*, vol. 13, no. 1, p. 1153, Jan. 2023.

[51] Y. Keshun, W. Chengyu, and L. Huizhong, "Research on intelligent implementation of the beneficiation process of shaking table," *Minerals Eng.*, vol. 199, Aug. 2023, Art. no. 108108.

WENLI SHANG received the M.S. degree from the School of Mechanical and Automation Engineering, Northeastern University, in 2002, and the Ph.D. degree from the Laboratory of Industrial Control Network and System, Shenyang Institute of Automation, Chinese Academy of Sciences, in 2005. From 2005 to 2019, he was an Assistant Researcher and an Associate Researcher with the Shenyang Institute of Automation, Chinese Academy of Sciences. Since 2020, he has been a Professor with Guangzhou University. His research interests include industrial control system information security, computational intelligence and machine learning, and edge computing.

TIANYU GONG received the M.S. degree in control science and engineering from Shenyang Jianzhu University, Liaoning, China, in 2020. Since 2020, he has been with the China Industrial Control Systems Cyber Emergency Response Team, Beijing, China. He is currently an Assistant Engineer with the China Industrial Control Systems Cyber Emergency Response Team. His current research interests include information security, vulnerability analysis, and vulnerability mining for industrial control systems.



JING HOU received the M.S. degree in control engineering from the University of Shenyang Jianzhu, Liaoning, in 2004, and the Ph.D. degree in pattern recognition and intelligent system from Northeastern University, Liaoning, China, in 2019. Since 2004, she has been with the Shenyang Jianzhu University, where she is currently an Associate Professor. Her current research interests include robot control, intelligent control algorithm, and micro-nano manipulations.

JIAYUE LU was born in Guangdong, China, in 1999. He is currently pursuing the Graduate degree in communication engineering with the School of Electronics and Communications Engineering, Guangzhou University, Guangzhou, China. His research interests include industrial control system information security and risk assessment.

ZHONG CAO received the M.S. degree from the School of Computer Science and Educational Software, Guangzhou University, in 2005, and the Ph.D. degree from the School of Energy Science and Engineering, University of Electronic Science and Technology of China, in 2015.

From December 2016 to December 2017, he was a Visiting Scholar with the Department of Civil and Environmental Engineering, University of North Carolina at Charlotte, Charlotte, NC, USA. He is currently a Teacher with the School of Electronics and Communications Engineering, Guangzhou University. His research interests include industrial control systems, information security, machine learning, and intelligence control.