Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees

Wenli Shang,1,2,3 Tianyu Gong,1,3,4 Chunyu Chen,1,2,3,4 Jing Hou,5 and Peng Zeng1,2,3,4

1Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China
2University of Chinese Academy of Sciences, Beijing 100049, China
3Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China
4Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110016, China
5Information and Control Engineering Faculty, Shenyang Jianzhu University, Shenyang 110168, China

Correspondence should be addressed to Wenli Shang; shangwl@sia.cn

Received 23 October 2018; Accepted 26 February 2019; Published 14 March 2019

Academic Editor: Kuo-Hui Yeh

Copyright © 2019 Wenli Shang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Information security risk assessment for industrial control system is usually influenced by uncertain factors. For effectively dealing with problem that the uncertainty and quantification difficulties are caused by subjective and objective factors in the assessment process, an information security risk assessment method based on attack tree model with fuzzy set theory and probability risk assessment technology is proposed, which is applied in a risk scenario of ship control system. Firstly, potential risks of the control system are analyzed and the attack tree model is established. Then triangular fuzzy numbers and expert knowledge are used to determine the factors that influence the probability of a leaf node and the leaf nodes are quantified to obtain the interval probability. Finally, the fuzzy arithmetic is used to determine the interval probability of the root node and the attack path. After defuzzification, the potential risks of the system and the probability of occurrence of each attack path are obtained. Compared with other methods, the proposed method can greatly reduce the impact of subjectivity on the risk assessment of industrial control systems and get more stable, reliable, and scientific evaluation results.

1. Introduction

Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) are important components of the modern industrial environment and critical infrastructure [1]. ICS and SCADA systems are widely used in petroleum, power, chemical, rail transport, and other industries [2]. With the rapid development of network technology and industrial automation technology, ICS and SCADA are gradually connected to the Internet. In the process of improving remote control efficiency, it exposes potential risks in the control network, increasing system security risks. According to RISI, the authoritative industrial security information database [3], there have been more than 200 attacks on ICS worldwide by 2010. In particular, Stuxnet [2] virus penetrated into Iran’s nuclear facilities, causing a large number of equipment to stop working. This incident has brought great concern to the network security of ICS and SCADA. In 2017, the security report [4] from the US Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) stated that the ICS-CERT has collected 427 vulnerabilities. Among them, there are 295 security vulnerabilities were exploited, causing ICS to be attacked by cyber-attacks. These network attacks directly lead to the failure of ICS, and even cause major security incidents, which cause serious consequences for personnel, equipment, and environment. Protecting ICS from cyber-attacks is critical to a country’s economic development and social stability. ICS’s network security problem must be taken seriously [5]. Information security risk assessment of industrial control systems can effectively help users to identify potential system risks and take appropriate defensive measures, which has become the focus of current industrial research.

The information security risk analysis process of ICS is mainly composed of three steps [6]: risk scenario identification, probability analysis, and impact analysis. The
risk scenario identification focuses on the research object, identifies system's weaknesses in specified risk scenario, and comprehensively assesses the potential risks of the system. The probability of potential risk of the system can be assessed by using expert knowledge or using the Common Vulnerability Scoring System (CVSS). Finally, adverse effects of risk on the system are determined according to the probability.

With the rapid development of information technology and industrial technology, modern ICS has higher complexity, flexibility, and openness than traditional ICS, which brings great challenges to information security risk assessment. Information security risk assessment usually needs the help of expert assessment, and how to carry out scientific evaluation has been a research hotspot. At present, great achievements in the risk assessment methods of ICS information security have been made by international experts and scholars. Yingying Jiang et al. [7] proposed a method of analytic hierarchy process (AHP) and fuzzy evaluation set to assess the risk of SCADA in oil and gas fields. Huikang Lu et al. [8] proposed an ICS information security risk assessment method based on fuzzy analytic hierarchy process. Although the two methods can reduce the influence of human subjective factors to some extent by using fuzzy analytic hierarchy process (FAHP), the two methods do not reflect the potential risks of the system and the attacker's behaviors, which affects the formulation of defensive measures. D Ren et al. [9] proposed a location privacy protection risk assessment method based on attack tree in vehicle VANET and Jianguo Rong et al. [10] proposed an attack tree based on wireless sensor network location privacy risk assessment. Although the two methods can evaluate the target system quantitatively and accurately, however, the corresponding weight calculation method is not specified in the process of risk assessment for leaf nodes. In addition, CheeWooi Ten et al. [11] proposed a method for evaluating network security vulnerabilities using attack trees and conducting risk assessment for SCADA systems in power control networks. Yeqi Ru et al. [12] proposed an AHP quantitative risk assessment method based on attack tree model and AHP to assess the impact of cyber-attacks on the entire electronic physical system. Dong et al. [13] established the CBTC system attack tree model to assess the rail transit control system. The above research results show that the attack tree is an effective mathematical model to judge the potential threats of the ICS system. However, the accuracy of ICS information security risk assessment will be affected by subjective factors in the process of quantification. Traditional probabilistic techniques neglect the uncertainty and difficulties in quantifying security incidents, which affect the reliability of assessment.

To address these problems, an information security risk assessment method based on attack tree model is proposed in this paper, which combines fuzzy theory and probabilistic risk assessment technology. Fuzzy set theory is applied to probabilistic risk assessment technology to solve the issue of quantifying uncertain events caused by subjective and objective factors. The case study of information security risk assessment of ship control system shows that the method can effectively reduce the uncertainty caused by subjective and objective factors, increasing the stability and reliability of evaluation results. The remainder of the paper is structured as follows. The second part introduces the relevant theoretical basis, including the introduction of ship control system, attack tree model theory, and fuzzy set theory. The third part elaborates the fuzzy theory and probabilistic risk assessment method based on attack tree model proposed in this paper. The fourth part is taking the ship control system as the analysis case. It proves the validity and positive determination of the proposed method. The fifth part is the conclusion and prospect of the research work.

2. Related Work

2.1. Ship Control System. The development of ship automation systems is mainly composed of three stages [14]: unit device automation, cabin automation, and integrated ship automation. Unit device automation is in the embryonic stage of ship automation. Due to the fact that unit device was limited by the technology of the time, there was no communication between instrument and external device. With the development of automation technology, distributed monitoring system appears in people's vision. Initially, the distributed monitoring system only uses one computer to achieve centralized monitoring, which has great risks. Once the computer fails, the whole ship will stop working. Subsequently, the distributed monitoring system gradually replaces the centralized monitoring system. However, the distributed monitoring system is closed, independent, low flexibility, and lack of unified management. With the advent of information sharing, network integration, and other technologies, the ship control system has gradually developed into a comprehensive, multilevel, structured management, and monitoring system, which achieve integrated ship automation control.

The distributed control system (Figure 1) usually consists of three layers [15]: management layer, monitoring equipment layer, and field control layer. The management layer realizes centralized control and management of the monitoring and control layer through the network connection. Field devices are connected by fieldbus technology or remote I/O unit, and information exchange with monitoring layer is realized by network connectors such as bus or gateway. The device monitoring layer monitors and collects data from devices in the field device layer, than transmitting data to the management layer for centralized management and analysis.

The integrated automation control system of ship maintains communication with the remote control center through satellites. In the process of completing navigation, network query, and other services, it uploads important parameters to the remote control center for control and management. However, with the development of industrial network technology, industrial networks are facing huge security threats and cyber-attacks are spreading which trend to develop in a distributed, complex, and large-scale. The more concealed and longer latency make network viruses, denial of service, and other attacks much more disruptive. The integrated automation control system of ship has a single communication method, a complex network structure, and a large of data flow, which is extremely vulnerable to attack. Therefore, the
risk assessment and protection of the ship control system is imminent.

2.2. Attack Tree Model. The earliest attack tree model [15] was proposed by Bruce Schneier, the professor of Carnegie Mellon University, in 1999. The attack tree model uses a tree structure to describe the attack behaviors, the attack path, and the interdependence between them. It can visually describe the potential risks of the system. The purpose of an attacker may be to steal important parameters related to ship control, and more importantly, to gain control rights of the ship control system to achieve the purpose of destruction. So risk assessment experts can use attack tree model to describe their attack behavior, analyze the vulnerability of attackers, and adopt specific attack paths, so as to propose corresponding defensive measures. However, the attacker is usually sensible. They will choose a means of attack means which is low cost, low attack difficulty, and difficult to detect to achieve the purpose of obtaining system control authority.

The attack tree model (Figure 2) is structured and hierarchically distributed which uses a bottom-up generation method. Each leaf node of the attack tree is connected to its parent node by an AND or OR node. An attacker starts with a leaf node that represents the vulnerability of the system and uses the corresponding logical operations to reach the final root node. The logical operator AND indicates that all leaf node conditions under the root node must be satisfied to achieve the purpose of attacking the root node. The OR node indicates that the purpose of attacking the root node can be achieved if any leaf node under the root node is satisfied.

2.3. Fuzzy Set Theory. Zadeh first proposed fuzzy set theory in 1965 [16]. He believes that the probability theory in the traditional sense is not enough to describe the uncertainty associated with conceptualization because expert knowledge is not absolute and there are some uncertain factors to some extent [16, 17]. In order to effectively deal with uncertainty or subjectivity effectively, fuzzy theory is widely used in various fields, including reliability analysis and risk assessment. In the process of analysis and evaluation, fuzzy numbers are usually used to express the uncertainty of events, which is an interval analysis form for solving uncertain or imprecise events. The fuzzy number describes the relationship between the probability $P$ of the occurrence of an uncertain event and the membership function $\mu \in [0, 1]$. Fuzzy set theory is an extension of traditional set theory. Any shape of fuzzy number is possible, but the selected shape should be determined by expert knowledge. Generally speaking, Triangular Fuzzy Numbers (TFN) have great flexibility and accuracy in the representation and propagation of uncertain events in models such as event trees, fault trees, and attack trees. We can use TFNs to represent the probability which...
are described by expert knowledge. Interval probability can be used to indicate the possibility of occurrence of event. The process includes the following steps [18]:

1. Use the TFNs to determine the probability of basic events.
2. Use the TFNs to determine the interval probability of the resulting event.
3. Defuzzify the interval probability to obtain the point estimation probability of the event.

Risk assessment experts often use possible, very possible, and impossible languages to express the probability of an event rather than directly using numbers to indicate the probability of an event [19]. As a result of the expert knowledge expresses the uncertainty of the event to a certain extent, TFNs are more suitable to be used to express the probability of event. TFN is a vector group \((p_l, p_m, p_h)\) consisting of three vectors ranging from 0 to 1, where \(p_l\) is the minimum probability of occurrence of the event, \(p_m\) is the probability of occurrence of the event, and \(p_h\) is the maximum probability of occurrence of the event. TFNs can be represented by a set of four tuples (formula (1)).

\[
\bar{P}(\alpha) = \{\alpha_i, p_l, p_m, p_h\} \quad i = 1, 2, \ldots, n
\]  

The formula corresponding to the typical TFN membership function image (Figure 3) is shown in

\[
\mu_p(p_e) = \begin{cases} 
\frac{p_e - p_l}{p_m - p_l} & p_l \leq p_e \leq p_m \\
\frac{p_h - p_e}{p_h - p_m} & p_m \leq p_e \leq p_h \\
0 & \text{otherwise}
\end{cases}
\]  

According to the expert knowledge, the factors affecting the occurrence of leaf node events in the attack tree are graded, and the influencing factors are described by five probability levels (Figure 4), which are low (VL), possible (L), moderate (M), high (H), and very high (VH).

3. Fuzzy Theory and Probabilistic Risk Assessment Method Based on Attack Tree Model

Information security risk analysis for ICS system mainly includes asset identification, threat identification, and vulnerability identification [20]. After determining the relationship among the three elements of risk analysis, the probability of security incidents can be accurately assessed. Formula (3) is a mathematical expression for the loss caused by the occurrence of a security event.

\[
R(A, T, V) = R(P(T, V), F(L_a, V_a))
\]  

where \(P\) is probability of security events caused by system vulnerabilities; \(T\) refers to the probability of occurrence of basic safety events; \(V\) refers to the vulnerability. \(F(L_a, V_a)\) is the loss of the asset value caused by the security event; \(L_a\) is the loss of the asset value; \(V_a\) is the level of vulnerability. From this, the risk value calculation formula can be defined. In formula (4), \(L_V\) is the asset value loss caused by acquiring the attack target and \(P_G\) is the probability of occurrence of the target node event.

\[
R = L_V \times P_G
\]  

Fuzzy arithmetic involves the division of fuzzy numbers, which includes addition, subtraction, and multiplication. The partition of fuzzy numbers is an important part of fuzzy arithmetic. There are usually two ways to perform the fuzzy arithmetic [21], calculated by extension or \(\alpha - cut\) principle. The risk assessment needs to directly reflect the probability of the potential risk in the system; consequently in this paper
the $\alpha - cut$ principle is selected to implement the fuzzy arithmetic. The attacker aims to obtain the control authority of the target which is the root node of attack tree. Firstly, the potential risks of the target system are analyzed and an attack tree model is established. Then the probability of influencing factors of leaf nodes is assessed. Finally the probability of basic events is calculated. The above process provides a great reference value for describing attack path intuitively, studying attack mechanism, and taking defensive measures. The specific process based on fuzzy theory and probabilistic risk assessment method proposed in this paper is as follows (Figure 5).

(1) The Quantization of Leaf Node Based on TFNs. The TNFs with a confidence degree of $(1 - \alpha)\%$ are used as the assessment standard. The probability of attributes that affect the occurrence of attack event on leaf nodes is assessed by expert knowledge to achieve the quantization of leaf nodes.

(2) The Probability of Leaf Node Events Based on TFNs. From the assessment criteria obtained in step (1), according to the multiattribute utility theory, the interval probability of attack tree leaf node events is calculated.

(3) Interval Probability and Defuzzification of Root Node Event Based on TFNs. After calculating the probability of leaf node events, the TFNs arithmetic and probability risk assessment method proposed in this paper are used to calculate the probability interval of attack tree root node events. In order to reflect the probability of event and to facilitate the calculation of the risk value of the final event, the point estimation probability of event is obtained by defuzzification. In the above process, the probability interval of the root node event obtained by using the TFNs arithmetic and the probabilistic risk assessment technology reflect the fact that security event is a kind of possibility incident. After defuzzification, the point estimation probability of security events has better stability and reliability.

(4) Attack Path and Risk Value Analysis of the Root Node. The value loss caused by intrusion is determined by the probability of root node event, and the final risk value is obtained according to the formula (4). The attack tree model intuitively reflects the process that the attacker takes certain steps to gradually obtain the control authority of the target system. The probability of attack paths is calculated to better grasp attackers' most likely intrusion methods.

3.1. The Quantization of Leaf Node Based on TFNs. Leaf nodes in attack trees represent vulnerabilities that attackers may exploit to attack root nodes. However, when an attacker exploits system vulnerabilities, the factors considered are not unique, such as the cost of the attack, the level of the vulnerability, and the probability of the attacker being detected. Although the attacker will make a preevaluation of the cost, difficulty, and discoverability before launching the attack, the assessment result will exceed or fall below the preevaluation index because of the influence of many factors, so there is great uncertainty in the attack event.

The ultimate purpose of the attacker is to gain control of the target. Generally speaking, the higher the attack cost, the lower the probability of occurrence; the more difficult the attack, the lower the probability of vulnerability utilization; the more difficult the attack is to detect, the higher the probability of occurrence is. Attackers will carefully consider the above factors and choose the best attack mode to achieve the ultimate goal. These three attributes are used to quantify the leaf nodes of attack trees. According to the expert knowledge, the uncertainty of the above three factors is evaluated by using triangular fuzzy numbers. The evaluation standards are shown in Table 1.

Formula (2) is used to calculate the membership function of TNFs which represent the uncertainty. $\tilde{P}_{\text{SBE}_{\text{attribute}}} (\alpha)$ is a TFN with $\alpha - cut$ level and confidence level of $(1 - \alpha)\%$ $(\alpha \in [0, 1])$. Formula (5) is used to calculate the possibility assessment standard with confidence of $(1 - \alpha)\%$.

$$\tilde{P}_{\text{SBE}_{\text{attribute}}} (\alpha) = [p_i + \alpha \times (p_m - p_i), p_h - \alpha \times (p_h - p_m)]$$

Table 1 is the standard fuzzy evaluation language and the corresponding TFNs. We need to process it using formula (5) to obtain an evaluation criterion with confidence of $(1 - \alpha)\%$. The expert knowledge is used to evaluate the attributes affecting the leaf nodes, and the probability of occurrence of the leaf node event is calculated.

3.2. The Probability of Leaf Node Events Based on TFNs. The probability of occurrence of leaf node events is affected by three attributes: attack cost, difficulty, and possibility of detection. According to the multiattribute utility theory, these three factors are applied to calculate the occurrence probability of leaf node events. The formula is shown as formula (6).

$$\tilde{P}_{\text{SBE}_i} (\alpha) = W_{\text{cost}} \times \tilde{P}_{\text{SBE}_{\text{cost}}}_i + W_{\text{diff}} \times \tilde{P}_{\text{SBE}_{\text{diff}}}_i + W_{\text{det}} \times \tilde{P}_{\text{SBE}_{\text{det}}}_i$$

where $i$ is an arbitrary node, indicating an attack event. $\tilde{P}_{\text{SBE}_i} (\alpha)$ is the interval probability of the leaf node event
with a confidence degree of \((1 - \alpha)\%\); \(\tilde{P}_{SBE_{cost}}\) is the interval probability of attack cost; \(\tilde{P}_{SBE_{diff}}\) is the interval probability of vulnerabilities being exploited; \(\tilde{P}_{SBE_{det}}\) is the interval probability for attack behavior detected. \(W_{cost}\) is the weight of attack cost; \(W_{diff}\) is the weight of attack difficulty and \(W_{det}\) is the weight of the attack behavior detected. And the following relationship is satisfied between the weights.

\[
W_{cost} + W_{diff} + W_{det} = 1
\]  

(7)

### 3.3. Interval Probability and Defuzzification of Root Node Events Based on TFNs

In the attack tree model, the leaf nodes and root nodes are connected by logical AND or OR nodes. Therefore, there are two ways to calculate the probability of root nodes from the leaf node upward. In the attack tree which consisted of OR nodes (Figure 2), formula \((8)\) is used to calculate the probability of the target node spacing of event \(\tilde{P}_G\).

\[
\tilde{P}_G(\alpha) = \max \tilde{P}_{BE_i}
\]

(8)

Formula \((9)\) is used to calculate the interval probability \(\tilde{P}_{BE}(\alpha)\) of the basic event \(SE_i\) which represents the father node of the leaf node.

\[
\tilde{P}_{BE_i}(\alpha) = 1 - \prod_{i=1}^{n} (1 - \tilde{P}_{SBE_i})
\]

(9)

where \(\tilde{P}_{BE}(\alpha)\) is the interval probability of the leaf node under the target node and \(\tilde{P}_{SBE_i}\) is the interval probability of the security basic event. Security basic events determine the occurrence of basic events.

In the attack tree which consisted of AND nodes, the interval probability \(\tilde{P}_{BE}\) of the father node event is calculated as shown in formula \((10)\). The interval probability calculation principle of attack tree root event \(\tilde{P}_G\) is also applicable to formula \((10)\).

\[
\tilde{P}_{BE}(\alpha) = \tilde{P}_{SBE_1} \times \tilde{P}_{SBE_2} \times \cdots \times \tilde{P}_{SBE_n}
\]

(10)

The fuzzy set theory uses the fuzzy arithmetic operations based on the \(\alpha\)-cut formulation to manipulate fuzzy numbers in the process of calculating the interval probability of target node events [21]. Suppose \(\tilde{P}_{SBE}(\alpha) = (p_{l_A}, p_{m_A}, p_{h_A})\) is a TFN which is representing the possibility of the occurrence of event \(SBE_A\). The multiplication and complement operations of event \(SBE_A\) are shown in formulas \((11)\) and \((12)\).

\[
\xi \times \tilde{P}_{SBE_A}(\alpha) = \xi \times (p_{l_A}, p_{m_A}, p_{h_A})
\]

\[
= (\xi \times p_{l_A}, \xi \times p_{m_A}, \xi \times p_{h_A})
\]

(11)

where \(\xi > 0, \xi \in R\)

\[
\tilde{P}_{SBE_A}(\alpha) = 1 - (p_{l_A}, p_{m_A}, p_{h_A})
\]

\[
= (1 - p_{l_A}, 1 - p_{m_A}, 1 - p_{h_A})
\]

(12)

### 3.4. Attack Path and Risk Value Analysis of the Root Node

It is also necessary to calculate the value loss caused by the system being invaded after analyzing the probability of the root node event. It can be known from formula \((4)\) that the risk value of the root node of the attack tree is equal to the occurrence probability of the target node event multiplied by the loss caused by the event. However, the value loss price is not only related to the loss of the system itself invaded, but also related to environmental losses, personnel safety, social impact, and other factors.

---

**Table 1: The possibility of evaluation criteria.**

<table>
<thead>
<tr>
<th>Attack Cost</th>
<th>Probability Interval</th>
<th>Attack Difficulty</th>
<th>Probability Interval</th>
<th>Detected Possibility</th>
<th>Probability Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>(0.00,0.12,0.24)</td>
<td>Very High</td>
<td>(0.00,0.12,0.24)</td>
<td>Very High</td>
<td>(0.00,0.12,0.24)</td>
</tr>
<tr>
<td>High</td>
<td>(0.19,0.31,0.43)</td>
<td>High</td>
<td>(0.19,0.31,0.43)</td>
<td>High</td>
<td>(0.19,0.31,0.43)</td>
</tr>
<tr>
<td>Medium</td>
<td>(0.38,0.50,0.62)</td>
<td>Medium</td>
<td>(0.38,0.50,0.62)</td>
<td>Medium</td>
<td>(0.38,0.50,0.62)</td>
</tr>
<tr>
<td>Low</td>
<td>(0.57,0.69,0.81)</td>
<td>Low</td>
<td>(0.57,0.69,0.81)</td>
<td>Low</td>
<td>(0.57,0.69,0.81)</td>
</tr>
<tr>
<td>Very Low</td>
<td>(0.76,0.88,1.00)</td>
<td>Very Low</td>
<td>(0.76,0.88,1.00)</td>
<td>Very Low</td>
<td>(0.76,0.88,1.00)</td>
</tr>
</tbody>
</table>
The loss of system assets includes data loss, hardware loss, and software loss. These are also affected by three security factors: confidentiality, integrity, and availability. The value of asset in a risk assessment is not a loss of value in the traditional sense but is determined by the degree of influence of the different levels of the three security attributes above. The system will cause additional asset value loss to the environment, personnel and society after being invaded. Therefore, it is necessary to assess the asset value loss of the system. In order to fully consider the damage caused by intrusion, formula (15) is used to define the mathematical expression of value loss \( L_V \) in this paper.

\[
L_V = \lambda \times \left( \alpha_1 DT_i + \beta_1 HW_i + \delta_1 SW_i \right) + \mu \\
\times \left( \alpha_2 E_i + \beta_2 H_i + \delta_2 S_i \right)
\]

(15)

where the weight satisfies \( \lambda + \mu = 1 \) and \( \alpha_1 + \beta_1 + \delta_1 = 1 \). \( DT_i \) is the loss of value of data assets; \( HW_i \) is the loss of value of hardware assets; \( SW_i \) is the loss of value of software assets; \( E_i \) is the loss of value of personnel assets; \( H_i \) is the loss of environmental value; \( S_i \) is the loss of social value.

The asset loss to the system caused by the network attack is unique to the system. In addition, environmental damage, human safety, and social impact caused by network attacks are affected by many factors. The above problems make the calculation of value loss very complicated, which requires us to do more in-depth research. Therefore, this paper only gives the expression of value loss, but does not calculate it.

The attack path is an attack process that attackers exploit the leaf node vulnerability to gain the control access of the target node. This paper analyzes seven attack paths based on physical attack, communication network attack, and computer software vulnerability. Assuming the set of attack paths \( AP(\alpha) = \{AP_1, AP_2, \cdots, AP_n\} \), the probability of the attack path is represented by formula (16).

\[
\bar{\Psi}_{AP_\alpha} = \prod_{i=1}^{n} \bar{P}_{SBE_i}
\]

(16)

The attack path clearly reflects the attack behavior of the attacker to achieve the target of the attacking root node. It provides great help to determine the risk of each component, analyze the attack mechanism, analyze the attack path, and take defensive measures.

4. Information Security Risk Assessment Case for Ship Control System Figures

The risk assessment of ship control system is carried out with the method of information security risk assessment proposed in this paper. Due to the complexity of ship integrated automation control network, the abstracted ship power control network is used as a risk scenario for analysis.

In the abstracted ship power control network (Figure 6), the monitoring equipment layer is connected to the management layer through the gateway G1 and is connected to the field device layer through the gateway G2 and G3. The engineering station analyzes the data collected from the equipment, then transmits it to the management layer, and saves in the historical database. The PLC1 mainly controls the flow rate of the fuel putting into the combustion chamber of the gas turbine and controls the volume of the intake air by controlling the rotation speed of the turbine. PLC2 transmits control parameters collected from flow meter FM1 and pressure sensor SEN1 to engineer station for processing and analyzing. The air which is cooled and liquefied is fully mixed with the fuel to combust after entering the combustion chamber. The mixture gas produced by combustion is discharged under the control of PLC3. In addition, PLC3 transmits the control parameters collected by flow meter FM2 and pressure sensor SEN2 to the engineer station for processing and analyzing. PLC4 controls the amount of water entering the gas turbine by controlling the valve and the water pump. In addition to the cooling air, it is also improving the power of the gas turbine.

Attackers can use network attacks and physical attacks to achieve the purpose of intrusion, control and even destruction of SCADA. The network attack can be realized by attacking the communication network or exploiting the vulnerability in the software of the ship control system. The attacker may be an internal crew member of the ship. They use external devices to establish links with slave stations and violently crack the management login password to directly control the system to achieve physical attacks. Remote attackers can attack management layer communication networks to achieve attack intentions. They can steal a large number of sensitive parameters of ship control system by cracking encryption algorithm. They also can use replay attack to improve data transmission delay, consume link bandwidth, and even cause the system to send wrong data or instructions. In addition, denial-of-service attacks by attackers in internal networks can affect the availability of devices. For attacking system software, remote attackers can use buffer overflow vulnerabilities in control controllers to execute arbitrary code or use vulnerabilities in mail systems to execute arbitrary code remotely to control the target system. Virus also poses a serious threat to the control system. Compared with traditional viruses, industrial viruses are very destructive. They can control the system software and execute commands instead of the system, which is fatal to the security of the control system. The most famous is the worm virus, which is injected into the system through the U disk. Firstly, worms use the vulnerabilities in the system to complete the self-installation, diffusion process and hide in the system. Subsequently, it acquires the control rights of SCADA and PLC, tampers with the control parameters, and makes the gas turbine parameters abnormal without being noticed. Ultimately, abnormal temperature and pressure changes of gas turbines lead to its abnormal operation or even shutdown.

By analyzing the function of each component of the system and the attacking behavior of the attacker, the attack tree model of the target system is established (Figure 7). According to the probability assessment given in Table 1, this paper uses 95% confidence (\( \alpha = 0.05 \)) to implement the fuzzy arithmetic in consideration of the reliability of the expert evaluation. Formula (5) is used to calculate the new evaluation criteria corresponding to the TFNs with a
95% confidence level, as shown in Table 2. According to the possibility scoring criteria in Table 2, the attributes of each leaf node in the attack tree are evaluated by expert knowledge. The probability of the attributes is shown in Table 3.

In order to further verify the validity and rationality of the evaluation method proposed in this paper, the attack path analysis method proposed in [12] is compared with the method proposed in this paper under the same evaluation level. Analytic hierarchy process is used to determine the corresponding weights of formula (6). The weights are 1/2, 1/3, and 1/6. The interval probability of leaf node events in this paper and the point estimate probability of leaf node event using the method in literature [12] are shown in Table 4.

Formulas (8)–(13) are used to calculate the interval probability of the parent node event of each leaf node in the attack tree. Formula (16) is used to calculate the interval probability of attack path events. The probability of attack path events calculated by the method proposed in this paper and the method proposed in literature [12] are shown in Table 5.

In order to compare the evaluation results of the two methods more intuitively, formula (14) is used to defuzzify
the interval probability of attack path events. The probability distribution of the point estimation probability obtained by the method proposed in this paper and the method proposed in literature [12] are shown in Figure 8. After defuzzification, we can use formula (4) and (15) to calculate the risk value (it is not the focus of this paper).

It can be seen from Table 5 that the probability of event occurrence calculated by the method in reference [12] is basically within the interval probability of event occurrence calculated by the method proposed in this paper. The difference is that there are some errors in attack paths AP2 and AP4 between the two methods, which objectively reflects the
Table 4: The probability of leaf node events.

<table>
<thead>
<tr>
<th>Security Basic Event</th>
<th>Interval Probability</th>
<th>Event probability of Literature [12]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In This Paper</td>
<td></td>
</tr>
<tr>
<td>SBE1</td>
<td>(0.3860,0.5000,0.6140)</td>
<td>0.4167</td>
</tr>
<tr>
<td>SBE2</td>
<td>(0.2910,0.4050,0.5190)</td>
<td>0.3333</td>
</tr>
<tr>
<td>SBE3</td>
<td>(0.2277,0.3417,0.4557)</td>
<td>0.3167</td>
</tr>
<tr>
<td>SBE4</td>
<td>(0.4810,0.5950,0.7090)</td>
<td>0.3750</td>
</tr>
<tr>
<td>SBE5</td>
<td>(0.4493,0.5633,0.6773)</td>
<td>0.4544</td>
</tr>
<tr>
<td>SBE6</td>
<td>(0.2593,0.3733,0.4873)</td>
<td>0.3194</td>
</tr>
<tr>
<td>SBE7</td>
<td>(0.2277,0.3417,0.4557)</td>
<td>0.2639</td>
</tr>
<tr>
<td>SBE8</td>
<td>(0.3227,0.4367,0.5507)</td>
<td>0.3056</td>
</tr>
<tr>
<td>SBE9</td>
<td>(0.3543,0.4683,0.5823)</td>
<td>0.4167</td>
</tr>
<tr>
<td>SBE10</td>
<td>(0.4493,0.5633,0.6773)</td>
<td>0.3889</td>
</tr>
<tr>
<td>SBE11</td>
<td>(0.4810,0.5950,0.7090)</td>
<td>0.4167</td>
</tr>
<tr>
<td>SBE12</td>
<td>(0.4177,0.5317,0.6457)</td>
<td>0.3194</td>
</tr>
<tr>
<td>SBE13</td>
<td>(0.5443,0.6583,0.7723)</td>
<td>0.4722</td>
</tr>
</tbody>
</table>

Table 5: Attack path and event probability.

<table>
<thead>
<tr>
<th>Attack Path</th>
<th>The Attack Path Composition</th>
<th>Step Count</th>
<th>Interval Probability</th>
<th>Event probability of Literature [12]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>In This Paper</td>
<td></td>
</tr>
<tr>
<td>AP1</td>
<td>SBE1BE2</td>
<td>2</td>
<td>(0.1123,0.2025,0.3187)</td>
<td>0.1389</td>
</tr>
<tr>
<td>AP2</td>
<td>BE5BE3BE2</td>
<td>5</td>
<td>(0.0831,0.1811,0.3322)</td>
<td>0.0473</td>
</tr>
<tr>
<td>AP3</td>
<td>SBE3BE3BE2</td>
<td>3</td>
<td>(0.2277,0.3417,0.4557)</td>
<td>0.3167</td>
</tr>
<tr>
<td>AP4</td>
<td>SBE4BE3BE2</td>
<td>3</td>
<td>(0.4810,0.5950,0.7090)</td>
<td>0.3750</td>
</tr>
<tr>
<td>AP5</td>
<td>SBE5BE4BE2</td>
<td>3</td>
<td>(0.4493,0.5633,0.6773)</td>
<td>0.4544</td>
</tr>
<tr>
<td>AP6</td>
<td>SBE6BE3BE2</td>
<td>3</td>
<td>(0.2593,0.3733,0.4873)</td>
<td>0.3194</td>
</tr>
<tr>
<td>AP7</td>
<td>SBE7BE3BE2</td>
<td>3</td>
<td>(0.2277,0.3417,0.4557)</td>
<td>0.2639</td>
</tr>
</tbody>
</table>

Figure 8: The chart of probability distribution statistical.

The unstable factors in the evaluation methods in [12]. It can be seen from the comparison of Figure 8 that the probability of occurrence of the event calculated in [12] is lower than the method proposed in this paper. The low assessment results are easily overlooked by information security workers, leading to irreversible consequences. The stable assessment probability can provide a more reliable guarantee for reducing the occurrence of adverse events.

The greater advantage of this paper is to combine the fuzzy set theory and the probabilistic risk assessment method to calculate the interval probability of the attack events, which emphasizes the uncertainty of attack events under the influence of various factors. Not only does the interval probability data obtained from the assessment reduce the impact of human subjectivity on the information security risk assessment for ICS, but interval estimation is more referential for information security assessment workers than point estimation. In addition, the probability of point estimation gets much more stable, reliable, and scientific after defuzzification through comparative experiments.

5. Conclusion

In this paper, an information security risk assessment method based on attack tree model with fuzzy theory and probability risk assessment technology is proposed, which is applied in a risk scenario of ship control system. The interval probability obtained by fuzzy arithmetic and risk probability technique can better reflect the uncertainty of attack events. After defuzzification, the probability of point estimation is more representative, stable, and reliable than the comparison literature. In addition, it can greatly reduce the impact of the uncertainties caused by subjective and objective factors on information security risk assessment, which provides a more stable reference value for analyzing the potential
risk of the system, studying the attack mechanism, and taking appropriate defensive measures. This paper uses a static evaluation method to assess and analyze the attack behaviors. Because the scale of the attack tree model will affect the evaluation results, and the static evaluation lacks good real-time. Therefore, the future work will focus on how to conduct a risk assessment of the ICS system using a dynamic approach.

**Data Availability**

The data used to support the findings of this study are available from the corresponding author upon request.

**Conflicts of Interest**

The authors declare that they have no conflicts of interest.

**Acknowledgments**

This work is supported in part by the National Natural Science Foundation of China “Research on Anomaly Detection and Security Awareness Method for Industrial Communication Behaviors” (61773368), State Grid Corporation Science and Technology Project (5211018001H), and Chinese Academy of Sciences Strategic Pilot Science and Technology Project (52110118001H), and Chinese Science Foundation of China “Research on Anomaly Detection and Security Awareness Method for Industrial Communication Behaviors” (61773368), State Grid Corporation Science and Technology Project (52110118001H), and Chinese Academy of Sciences Strategic Pilot Science and Technology Project (52110118001H). The authors would also like to acknowledge the helpful comments and suggestions of the industry control system security software group. Their efforts are greatly appreciated.

**References**


