IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 19, 2022, accepted April 15, 2022, date of publication April 21, 2022, date of current version April 28, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3169133

Cybersecurity Risk Assessment of Industrial Control Systems Based on Order-α Divergence Measures Under an Interval-Valued Intuitionistic Fuzzy Environment

HUIJUAN GUO[1], LEI DING[2], AND WENCHAO XU[1]
[1]School of Information Engineering, Tianjin University of Commerce, Tianjin 300134, China
[2]Information Center of the Civil Aviation Administration of China, Beijing 100710, China

Corresponding author: Huijuan Guo (guohuijuan@tjcu.edu.cn)

This work was supported by the Tianjin Education Commission Scientific Research Project: Research on the Development of Collaborative Innovation under the Background of the Integration of Production and Education in Colleges under Grant 2018SK094.

ABSTRACT With the increasing deployment of network technologies in industrial control systems (ICSs), cybersecurity has become a challenge in ICSs. Cybersecurity risk assessment (CRA) plays an important role in cybersecurity protection of ICSs. However, the weights of risk indices are constants in traditional CRA methods, and they do not fully consider the requirements of risk identification. In this paper, we define a novel order-α divergence measure for interval-valued intuitionistic fuzzy numbers (IVIFNs) and further develop a novel CRA approach for ICSs based on the proposed divergence measure under an interval-valued intuitionistic fuzzy environment to contribute to the research gap. First, an order-α divergence measure for IVIFNs is defined considering flexibility and robustness of divergence measures with the parameter. Next, a variable weight-based CRA approach for ICSs is developed. In this approach, IVIFNs are adopted to describe evaluation values of risk indices. The weights of risk indices are variable weight vectors and they are determined by the relative divergence closeness. Integration approaches of each node and each attack path in attack-defense trees (ADTs) are proposed based on the operations of IVIFNs, and risk scores of each attack path are calculated by using the score function. Finally, we apply the proposed method to the CRA of a civil aviation fuel supply automatic control system and verify its effectiveness and advantages by comparing it with other methods. This method can dynamically adjust the weights of risk indices considering the relationship between each risk index and the highest risk, and therefore, it can more effectively recognize the highest risk of ICSs than the traditional CRA method. In addition, it can also match the risk attitude of decision-makers by adjusting the parameter α.

INDEX TERMS Industrial control systems (ICSs), cybersecurity risk assessment (CRA), order-αdivergence measure, interval-valued intuitionistic fuzzy numbers (IVIFNs), variable weight vectors.

I. INTRODUCTION

Industrial control systems (ICSs) are widely used in electric power, petroleum and petrochemical, nuclear energy, aviation, railway, water treatment and other industries. They play an important role in today's industry [1]. In recent decades, the progress of computer and network technology has promoted the development of ICSs [2]. For example, the Internet of Things has entered ICSs to achieve connectivity among enterprises and savings of cost. The integration of advanced information technology and ICSs can realize the remote control and monitoring of field equipment [3]. However, advanced technology not only brings some advantages to ICSs but also makes ICSs more vulnerable and subject to various network attacks. For instance, hackers and criminal organizations use the loopholes of ICSs to destroy the normal operation of ICSs in various ways and cause great impact and loss to society and the economy. We know that the

The associate editor coordinating the review of this manuscript and approving it for publication was Hualong Yu.

"Stuxnet" virus, which swept the world's industries in 2010, used the loopholes of Windows system and SIMATIC WinCC of Siemens to attack ICSs so that the centrifuge in Iran ran out of control, covered up the failure, and sent back to the management department with "normal operation" records, which resulted in misjudgment of decision-making [4]. In 2015, the virus called blackenergy attacked an energy company in the Ivano frankisvik region of western Ukraine, which led to the power failure of 225,000 families in Ukraine. Since May 12, 2017, the variant Wannacry Blackmail virus has swept the world, and some governments, airports, hospitals, gas stations and other public institutions have been attacked. In 2018, one chip manufacturing enterprise in Taiwan was also attacked by Wannacry Blackmail virus. All kinds of documents and databases were locked, which led to the shutdown of production lines. Although the number of attacks against ICSs is small compared with that against the internet, the consequences may be disastrous. Therefore, it is very important to ensure that ICSs are protected from cyber threats [5].

Aiming at cybersecurity problems, a series of standards have been formulated. ISO/IEC 27000 series standards on information security management solve the security problems of IT systems. The ISA/IEC 62443 standard provides a flexible framework to solve and mitigate the current and future security vulnerabilities in ICSs [6]. However, the cybersecurity problems of ICSs are difficult to eradicate. First, the standards of industrial control networks are mostly open to facilitate the application of users. As a result, it is not difficult for programmers familiar with the ICS to develop targeted malicious attack codes. In addition, the technology of hackers and criminal organizations is also improving, and it is difficult for ICSs to be free from network attacks. Risk assessment can help enterprises find the weakest links of ICSs and further take corresponding measures to optimize management, equipment and control [7]. Therefore, it is necessary to evaluate the cybersecurity risks of ICSs.

Quantitative risk assessment is an effective method of CRA. Some related works have been performed to assess cybersecurity risks of ICSs by exploiting different methods. For example, Li *et al.* [8] used a Petri net (PN) to establish an evaluation model and proposed a dynamic impact assessment method based on the full recognition of asset knowledge. Gemini and Sabu [9] presented a CRA method of the industrial internet of things (IoT) considering the largest loss stream based on an attack graph. Wang *et al.* [10] developed a CRA method combining the factor analysis of information risk (FAIR) model with Bayesian networks (BNs). From the accuracy-based perspective, they performed an in-depth analysis between FAIR and FAIR-BN under different situations based on the J-divergence measure. Qin *et al.* [11] designed an association network (AN) to infer the probabilities of cybersecurity incidents and built an association matrix with regard to the state variables and the key security variables to evaluate the cybersecurity risks of ICSs. According to the characteristics of risk assessment of power system, Sun *et al.* [12] proposed an incremental variable-based state enumeration method considering safety margins. Bolbot *et al.* [13] devised a risk assessment method for ship systems based on cyber preliminary hazard analysis. Chang *et al.* [14] applied a failure mode and effect analysis model to quantify the risk level combining evidential reasoning (ER) with a rule-based Bayesian network (RBN). Jha *et al.* [15] presented a risk assessment framework for smart grids, which applied hardware reliability and data reliability to evaluate risks.

Due to the limited prior knowledge of attacks, it is difficult for decision-makers to accurately evaluate the probabilities of attack events. Some researchers have implemented fuzzy theory into risk assessments of diverse fields, such as manufacturing corporations [16], construction project investment [17], traffic congestion [18], buildings [19], freight transportation systems [20], ship control systems [21], mines [22], and so on. The assessment data were expressed in their favor, such as fuzzy numbers [23]–[25], [30]–[32], intervals [33], [34], Z-numbers [35], triangular fuzzy numbers [16], [19]–[22], [26], [27], [36], trapezoidal fuzzy numbers [28], Pythagorean fuzzy numbers [37]–[40], linguistic term sets [17], [29], and double hierarchy hesitant fuzzy linguistic information [18]. In recent years, researchers have studied risk assessment from different technical models, different methods and different fuzzy evaluations. Wang *et al.* [18] combined double hierarchy hesitant fuzzy linguistic term sets with the ORESTE method and proposed a risk assessment method on the 5S traffic congestion model. Huang *et al.* [23] adopted entropy weights to calculate the relative importance of element layers in the fuzzy analytic hierarchy process (FAHP) model and improved the correlation between failure modes using the gray relation analysis (GRA) method. Considering the lack of sufficient historical data, Qi *et al.* [25] proposed a dynamic CRA method for ICSs by extending the traditional BN to a fuzzy BN. Gul *et al.* [26] combined a FAHP method with fuzzy VIKOR to construct a new risk assessment framework. Gul and Celik [27] proposed a risk assessment method by incorporating a fuzzy rule-based expert system with the Fine-Kinney method and applied it in rail transportation systems. Considering decision-makers' psychological behavior, interaction relationships, and uncertainty among risk indices, Wang *et al.* [28] presented a hybrid failure mode and effect analysis (FMEA) framework by combining the TODIM approach with the Choquet integral method. Li *et al.* [29] proposed a novel FMEA model taking linguistic term sets into account in fuzzy Petri nets (FPNs), which calculated the weights of decision-makers based on the TOPSIS method. Yu *et al.* [31] applied the cloud model to elaborate the risk indices, and the risk indices were integrated by the MAX-MIN operator. Ultimately, the method provided the risk levels under different situations, and a detailed and in-depth discussion was made. From the author's point of view, the randomness of the cloud model is very strong, which will lead to different calculation results even though the same input values are given. Tian *et al.* [33] advanced a risk assessment method considering intervals with

self-confidence. In the approach, the weights of decision-makers were calculated by combining the subjective weights with the objective weights, and the fuzzy inference laid the foundation for IF-THEN rules. Onari *et al.* [35] introduced the Z-number theory to risk assessment. In this approach, the risk indices including severity, occurrence, and detection, are expressed by Z-numbers. However, the operations for Z-numbers are difficult, and we need to convert Z-numbers to other fuzzy numbers for further processing. Wang *et al.* [36] implemented attack-defense tree models (ADTs) for CRA of an airport automatic fuel supply control system based on fuzzy theory. Akram *et al.* [38] provided a risk evaluation under a Pythagorean fuzzy environment using hybrid TOPSIS and the ELECTRE I method. Recently, some novel Pythagorean fuzzy interaction aggregation operators based on Archimedean t-conorm and t-norm (ATT) have been developed [40], and applying them to CRA of ICSs will be a good subject.

Although existing fuzzy risk assessment methods manage uncertainty to some extent, Atanassov and Gargov [41] introduced the concept of the interval-valued intuitionistic fuzzy set (IVIFS), which is more powerful in expressing uncertainty. The operations for the IVIFS have been defined [42]–[44]. The fundamental characteristic of the IVIFS is that the values of its membership degree and nonmembership degree are intervals rather than exact numbers. Therefore, the IVIFS is finer and smoother for representing the fuzzy evaluation information than the fuzzy set (FS) and intuitionistic fuzzy set (IFS). Recently, it has still attracted the focus of scholars [45]–[51]. Liu *et al.* [45] obtained variable weights of attributes by integrating the accuracy function and the subjective weights; on this basis, a novel multi-attribute group decision-making (MAGDM) approach was developed with IVIFS. Garg and Kumar [46] presented some exponential distance measures using the connection number (CN) of IVIFS. Kumar and Chen [47] proposed a novel score function of CN based on set pair analysis (SPA) theory under an interval-valued intuitionistic fuzzy information environment. Che *et al.* [48] constructed a new entropy measure in the context of IVIFS by introducing the proposed distance function. Zhou *et al.* [49] raised the ratio comparison rules of IVIFS. Bustince *et al.* [50] introduced some new similarity measures between interval-valued intuitionistic fuzzy numbers (IVIFNs) considering the width of intervals and admissible orders. Deveci *et al.* [51] proposed a new combinative distance-based ASsesment (CODAS) method based on Taxicab distance and the largest Euclidean distance between the IVIFNs. Information measure is an important topic in fuzzy decision-making problems. Bhandari and Pal [52] defined the fuzzy divergence measure and provided a new fuzzy measure method from the perspective of probability distribution. Since then, scholars have conducted extensive research on this topic [53]–[63]. In recent years, Wang and Wan [58] transformed IVIFS into IFS, defined a possibility degree of IVIFS and developed a divergence measure for IVIFNs based on the proposed possibility degree. Li *et al.* [59] presented a new cross-entropy measure with parameters for IVIFNs based on the J-divergence measure. Mishra *et al.* [60] defined the Jensen-logarithmic divergence measure and the Jensen-exponential divergence measure for IVIFNs. Mishra *et al.* [61] defined some novel entropy and divergence measures, and applied them in the process of multicriteria service quality assessment combined with the TODIM method. Song *et al.* [62] introduced a divergence-based cross entropy measure with parameters for AIFSs, which is the intuitionistic fuzzy set defined by Atanassov and generally is also called IFS. Verma [63] advanced some new order-α divergence measures between two IFSs.

By combining the literature on risk assessment and IVIFNs, we are committed to developing a new CRA method for ICSs and a new fuzzy divergence measure under an interval-valued intuitionistic fuzzy environment for the following reasons:

1. The weights of risk indices are constants and do not vary with actual situations in the existing risk assessment methods. The weights of risk indices are determined by decision-makers considering their experience or determined by the entropy weight method. However, the constant-weighting approaches are unreasonable in the following situation. For example, it is easy to ignore the risk in this situation when the value of an index is very close to the highest risk and yet its weight is very small. However, the risks of ICSs easily cause serious consequences. Therefore, it is necessary to develop a new assignment method for the weights of risk indices.

2. FS only reflects the membership degree of belonging to one level. IFS embodies the membership degree of belonging to one level and the nonmembership degree of not belonging to one level. For FS and IFS, their membership degrees and nonmembership degrees are expressed by exact numbers. However, due to the limitations of the decision-maker's experience and uncertainty of risk indices, it is difficult for decision-makers to evaluate risk indices belonging to one level and not belonging to one level with exact numbers. IVIFS can better describe uncertainty because its membership degree and nonmembership degree are intervals.

3. The divergence measure with the parameter has the characteristics of flexibility and robustness, yet there is a lack of research on it for IVIFNs.

Therefore, to address these issues, we define a novel order-α divergence measure for IVIFNs, and on this basis, we put forward a variable weight-based CRA method for ICSs under an interval-valued intuitionistic fuzzy environment. It arises from the ADT model. First, a novel divergence measure for IVIFNs is defined, and the weights of risk indices are calculated based on the proposed divergence measure. Second, a novel CRA method is established. Finally, the proposed method is applied to the CRA of a civil aviation fuel supply automatic control system, and its effectiveness is verified.

The main contributions of this paper are as follows:

1. We define a divergence measure with the parameter for IVIFNs. It makes up for the gap that there is no divergence measure with parameters for IVIFNs.
2. We expand IVIFS to the CRA of ICSs considering the power of IVIFS and formulate integration approaches of all nodes and attack paths with IVIFNs in the ADT model.
3. We develop a novel CRA method for ICSs. In this method, the weights of risk indices can vary with actual situations in the risk assessment process and are calculated by using the proposed divergence measure.

The rest of this article is organized as follows: Section II reviews the concept of the ADT model and theory about IVIFS. Section III defines a novel order-α divergence measure for IVIFNs. Section IV describes the framework and implementation process of our proposed approach. In addition, it introduces the risk assessment scales with IVIFNs, the determination method for the weights of risk indices, and the integration expressions of all nodes and attack paths based on the operations of IVIFNs. Section V introduces a case involving the CRA of a civil aviation fuel supply automatic control system and makes a comparative analysis with other methods. Section VI summarizes our work, states the contributions and limitations of the proposed method, and expounds further work.

II. PRELIMINARIES

A. ATTACK-DEFENSE TREES

In 1999, Schneier [64] proposed attack trees (ATs) as a tool to evaluate the security of complex systems. Considering the limitation of ATs that they cannot reflect the interaction between attacks and defenses, Kordy *et al.* [65] extended ATs to attack-defense trees (ADTs), which constitute a graphical expression of the actions that attackers might take to attack one system and the defenses that defenders can adopt to protect the system. An ADT model is a tree-like graph of an attack scenario, as shown in Fig. 1.

It consists of one root node, attack leaf nodes, defense leaf nodes and combination nodes. The attack target is defined as the root node, the attack leaf nodes are the actions to be implemented by attackers, and defense leaf nodes are the measures to be taken by defenders. In Fig. 1., G0 represent the root node, L1, L2, and L3 represent the attack leaf nodes, and D1, D2, and D3 represent the defense nodes. In addition, combination nodes consist of AND nodes and OR nodes. AND nodes indicate different steps to attack the same goal, and OR nodes are alternatives. Any path from leaf nodes to the root node indicates a complete attack process to realize the attack target. All attack paths can be generated by traversing the whole attack tree.

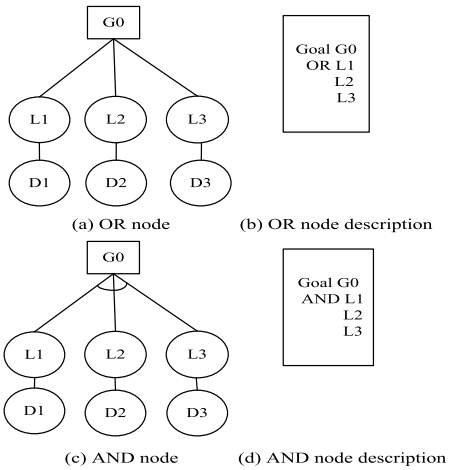

FIGURE 1. The representation of an ADT model.

B. THEORY ABOUT INTERVAL-VALUED INTUITIONISTIC FUZZY SET

Definition 1 [41]: Let X be a nonempty set, and then the interval-valued intuitionistic fuzzy set (IVIFS) is defined as

$$A = \left\{ x, \left(\left[\mu_A^L(x), \mu_A^H(x) \right], \left[\nu_A^L(x), \nu_A^H(x) \right] \right) \middle| x \in X \right\} \tag{1}$$

where $\mu_A^L(x)$ and $\mu_A^H(x)$ represent the upper and lower bounds of the membership degree, respectively, and $\mu_A^L(x), \mu_A^H(x) \subseteq [0,1]$. $\nu_A^L(x)$ and $\nu_A^H(x)$ represent the upper and lower bounds of the nonmembership degree, respectively, $\nu_A^L(x), \nu_A^H(x) \subseteq [0,1]$, and $\mu_A^H(x) + \nu_A^H(x) \leq 1$. $\pi_A^L(x)$ and $\pi_A^H(x)$ represent the upper and lower bounds of the hesitation degree, respectively, $\pi_A^L(x) = 1 - \mu_A^H(x) - \nu_A^H(x)$, $\pi_A^H(x) = 1 - \mu_A^L(x) - \nu_A^L(x)$.

The IVIFN $\left(\left[\mu_A^L(x), \mu_A^H(x) \right], \left[\nu_A^L(x), \nu_A^H(x) \right] \right)$ is expressed as $\left(\left[\mu_A^L, \mu_A^H \right], \left[\nu_A^L, \nu_A^H \right] \right)$ for convenience.

Definition 2 [42], [43]: Let $\alpha_1 = \left(\left[\mu_1^L, \mu_1^H \right], \left[\nu_1^L, \nu_1^H \right] \right)$ and $\alpha_2 = \left(\left[\mu_2^L, \mu_2^H \right], \left[\nu_2^L, \nu_2^H \right] \right)$ be any two IVIFNs, then the operations of IVIFNs are defined as

$$\begin{aligned}
\alpha_1 \oplus \alpha_2 = \Bigg(& \left[1 - \left(1 - \mu_1^L\right)\left(1 - \mu_2^L\right), \right. \\
& \left. 1 - \left(1 - \mu_1^H\right)\left(1 - \mu_2^H\right) \right], \\
& \left[\nu_1^L \times \nu_2^L, \nu_1^H \times \nu_2^H \right] \Bigg); \\
\alpha_1 \otimes \alpha_2 = \Bigg(& \left[\mu_1^L \times \mu_2^L, \mu_1^H \times \mu_2^H \right], \\
& \left[1 - \left(1 - \nu_1^L\right)\left(1 - \nu_2^L\right), \right. \\
& \left. 1 - \left(1 - \nu_1^H\right)\left(1 - \nu_2^H\right) \right] \Bigg); \\
\alpha_1 \cap \alpha_2 = \Bigg(& \left[\min\left(\mu_1^L, \mu_2^L\right), \min\left(\mu_1^H, \mu_2^H\right) \right], \\
& \left[\max\left(\nu_1^L, \nu_2^L\right), \max(\nu_1^H, \nu_2^H) \right] \Bigg);
\end{aligned}$$

$$\alpha_1 \cup \alpha_2 = \left(\left[\max\left(\mu_1^L, \mu_2^L\right), \max\left(\mu_1^H, \mu_2^H\right)\right], \left[\min\left(\nu_1^L, \nu_2^L\right), \min(\nu_1^H, \nu_2^H)\right]\right);$$

$$\lambda\alpha_1 = \left(\left[1-\left(1-\mu_1^L\right)^\lambda, 1-\left(1-\mu_1^H\right)^\lambda\right], \left[\left(\nu_1^L\right)^\lambda, \left(\nu_1^H\right)^\lambda\right]\right), \quad \lambda \succ 0;$$

$$\alpha_1^\lambda = \left(\left[\left(\mu_1^L\right)^\lambda, \left(\mu_1^H\right)^\lambda\right], \left[1-\left(1-\nu_1^L\right)^\lambda, 1-\left(1-\nu_1^H\right)^\lambda\right]\right), \quad \lambda \succ 0;$$

$$\alpha_1^c = \left(\left[\nu_1^L, \nu_1^H\right], \left[\mu_1^L, \mu_1^H\right]\right).$$

Definition 3 [66]: Let $A = \left(\left[\mu_A^L, \mu_A^H\right], \left[\nu_A^L, \nu_A^H\right]\right)$ be an IVIFN, and then its score function $S(A)$ is defined as

$$S(A) = \frac{1}{2}\left(\mu_A^L + \mu_A^H + \frac{\mu_A^H + \nu_A^H}{2}\left(1 - \mu_A^L - \nu_A^L\right) + \frac{\mu_A^L + \nu_A^L}{2}\left(1 - \mu_A^H - \nu_A^H\right)\right) \tag{2}$$

where $S(A) \in [0, 1]$.

III. A NOVEL DIVERGENCE MEASURE FOR IVIFNs

A. EXISTING DIVERGENCE MEASURES

Wang and Wan [58] gave a standard definition of divergence measures for IVIFSs below.

Definition 4 [58]: Let X be a finite universe, and let *IVIFS*s (X) be the set of all IVIFSs on X. A mapping D: *IVIFS*s $(X) \times$ *IVIFS*s $(X) \to [0, 1]$ is a standard divergence measure for IVIFSs if for every $A, B \in$ *IVIFS*s (X) which has the following properties:

(DP1) $D(A \| B) = 0$ if and only if $A = B$.
(DP2) $0 \le D(A \| B) \le 1$.
(DP3) $D(A \| B) = D(B \| A)$.

First, we review some recent divergence measures for IVIFNs.

Wan and Wang [58]:

$$D_W(A \| B) = \sqrt{\int_0^1 \int_0^1 [p(a \ge b) - p(A \ge B)]^2 \, d_\delta d_\beta}$$

where $a = (\mu_A, \nu_A) = \left(\mu_A^L + \delta\left(\mu_A^H - \mu_A^L\right), \nu_A^L + \beta\left(\nu_A^H - \nu_A^L\right)\right)$ and $b = (\mu_B, \nu_B) = \left(\mu_B^L + \delta\left(\mu_B^H - \mu_B^L\right), \nu_B^L + \beta\left(\nu_B^H - \nu_B^L\right)\right)$ with $\delta, \beta \in [0, 1]$.

$$p(a \ge b) = \max\left\{1 - \max\left\{\frac{1 - \nu_B - \mu_A}{2 - \mu_A - \nu_A - \mu_B - \nu_B}, 0\right\}, 0\right\},$$

$$p(A \ge B) = \int_0^1 \int_0^1 p(a \ge b) d_\delta d_\beta.$$

Li *et al.* [59]:

$$D_L(A \| B) = \frac{1}{\gamma - 1}\left[\left(\frac{m_A + m_B}{2}\right)^\gamma - \frac{1}{2}\left(m_A^\gamma + m_B^\gamma\right)\right]$$

where $m_A = \left(\mu_A^L + \mu_A^H + 2 - \nu_A^L - \nu_A^H\right)/4$, $m_B = \left(\mu_B^L + \mu_B^H + 2 - \nu_B^L - \nu_B^H\right)/4$, $\gamma \in (1, 2]$.

Mishra *et al.* [60]:

$$D_{M1}(A \| B) = 1 - \log_2\left(1 + \frac{1}{2}\begin{pmatrix}\min\left\{\mu_A^L, \mu_B^L\right\} + \min\left\{\mu_A^H, \mu_B^H\right\} + \\ \min\left\{\nu_A^L, \nu_B^L\right\} + \min\left\{\nu_A^H, \nu_B^H\right\} + \\ \min\left\{\pi_A^L, \pi_B^L\right\} + \min\left\{\pi_A^H, \pi_B^H\right\}\end{pmatrix}\right)$$

$$D_{M2}(A \| B) = \begin{cases} \dfrac{1}{1 - e^{-1/2}}\left(\dfrac{1}{2}\begin{pmatrix}\exp\left(-\left(\dfrac{\nu_A^L + \nu_A^H + 2 - \mu_A^L - \mu_A^H}{4}\right)\right) \\ + \exp\left(-\left(\dfrac{\nu_B^L + \nu_B^H + 2 - \mu_B^L - \mu_B^H}{4}\right)\right)\end{pmatrix} - \exp\left(-\dfrac{1}{8}\begin{pmatrix}\nu_A^L + \nu_A^H + \nu_B^L + \nu_B^H + 4 \\ -\mu_A^L - \mu_A^H - \mu_B^L - \mu_B^H\end{pmatrix}\right)\right) \\ \quad \text{if } \mu_A^L + \mu_A^H \ge \nu_A^L + \nu_A^H \\ \dfrac{1}{1 - e^{-1/2}}\left(\dfrac{1}{2}\begin{pmatrix}\exp\left(-\left(\dfrac{\mu_A^L + \mu_A^H + 2 - \nu_A^L - \nu_A^H}{4}\right)\right) \\ + \exp\left(-\left(\dfrac{\mu_B^L + \mu_B^H + 2 - \nu_B^L - \nu_B^H}{4}\right)\right)\end{pmatrix} - \exp\left(-\dfrac{1}{8}\begin{pmatrix}\mu_A^L + \mu_A^H + \mu_B^L + \mu_B^H + 4 \\ -\nu_A^L - \nu_A^H - \nu_B^L - \nu_B^H\end{pmatrix}\right)\right) \\ \quad \text{if } \mu_A^L + \mu_A^H \prec \nu_A^L + \nu_A^H \end{cases}$$

Mishra *et al.* [61]:

$$\begin{aligned} D_M(A \| B) = {} & \mu_A^L \ln \frac{\mu_A^L}{\left(\mu_A^L + \mu_B^L\right)/2} + \mu_A^H \ln \frac{\mu_A^H}{\left(\mu_A^H + \mu_B^H\right)/2} \\ & + \nu_A^L \ln \frac{\nu_A^L}{\left(\nu_A^L + \nu_B^L\right)/2} + \nu_A^H \ln \frac{\nu_A^H}{\left(\nu_A^H + \nu_B^H\right)/2} \\ & + \mu_B^L \ln \frac{\mu_B^L}{\left(\mu_A^L + \mu_B^L\right)/2} + \mu_B^H \ln \frac{\mu_B^H}{\left(\mu_A^H + \mu_B^H\right)/2} \\ & + \nu_B^L \ln \frac{\nu_B^L}{\left(\nu_A^L + \nu_B^L\right)/2} + \nu_B^H \ln \frac{\nu_B^H}{\left(\nu_A^H + \nu_B^H\right)/2} \end{aligned}$$

Now, we advance two examples to illustrate the weaknesses of the above developed divergence measures for IVIFNs. The calculation results are shown in Table 1.

It can be seen from Table 1 that the divergence value between A and B is 0 by using the divergence measure in [58] when the IVIFN A is $([0.3, 0.3], [0.6, 0.6])$ and the IVIFN B is $([0.2, 0.2], [0.3, 0.3])$. Obviously, A is not equal to B. In other words, when two IVIFNs degenerate into two IFNs, the divergence measure in [58] violates the property DP1. Divergence values between A and B are all 0 by using the divergence measure D_L in [59] and the divergence measure D_{M2} in [60] when A is $([0.3, 0.5], [0.3, 0.5])$ and B is $([0.2, 0.3], [0.2, 0.3])$. That is, when the distributions of the membership degree are the same as those of the nonmembership degree for two IVIFNs,

TABLE 1. Divergence values under different divergence measures.

	A=([0.3,0.5],[0.3,0.5]), B=([0.2,0.3],[0.2,0.3])	A=([0.3,0.3],[0.6,0.6]), B=([0.2,0.2],[0.3,0.3])
Divergence in [58]	$D_W(\mathrm{A}\|B)=0.030$	$D_W(\mathrm{A}\|B)=0$
Divergence in [59]($\gamma=1.5$)	$D_L(\mathrm{A}\|B)=0$	$D_L(\mathrm{A}\|B)=0.003$
Divergence in [59]($\gamma=2$)	$D_L(\mathrm{A}\|B)=0$	$D_L(\mathrm{A}\|B)=0.003$
Divergence in [60]	$D_{M1}(\mathrm{A}\|B)=0.234$ $D_{M2}(\mathrm{A}\|B)=0$	$D_{M1}(\mathrm{A}\|B)=0.322$ $D_{M2}(\mathrm{A}\|B)=0.001$
Divergence in [61]	$D_M(\mathrm{A}\|B)=0.071$	$D_M(\mathrm{A}\|B)=0.122$

it is not suitable to use them to calculate the divergence, and they do not meet the property DP1 of the divergence measure for IVIFNs. The divergence calculated by using the divergence measure D_{M1} in [60] and the divergence measure D_M in [61] is reasonable. However, we note that the divergence measure with parameters for IVIFNs is still a gap, which can provide better flexibility and robustness in real decision-making problems. Therefore, in the following, we are determined to develop a divergence measure with parameters for IVIFNs.

B. A NOVEL DIVERGENCE MEASURE FOR IVIFNs

First, we present three Lemmas in which we provide some support for developing the order-α divergence measure for IVIFNs.

Lemma 1: Let two finite discrete probability distributions be $P=(\mathrm{p}_1,p_2,\cdots,p_t)$ and $Q=(\mathrm{q}_1,q_2,\cdots,q_t)$, $0\le p_{\mathrm{k}}, q_{\mathrm{k}}\le 1$ for $\mathrm{k}=1,2,\cdots,t$, and $\sum_{\mathrm{k}=1}^{t}p_{\mathrm{k}}=\sum_{k=1}^{t}q_{\mathrm{k}}=1$.

If f_c is a mapping, $f_c:[0,1]\times[0,1]\to[0,1]$. For $\alpha\in[0,1]$,

$$f_c(P,Q)=\sum_{\mathrm{k}=1}^{t}p_{\mathrm{k}}^{\alpha}\left(\frac{p_{\mathrm{k}}+q_{\mathrm{k}}}{2}\right)^{1-\alpha}\le 1 \tag{3}$$

and the equality in (3) holds if and only if$p_{\mathrm{k}}=q_{\mathrm{k}}$, $\forall$k.

Proof of Lemma 1: Consider the function $\phi(x)=x^{1-\alpha}$ for every $x\in[0,\infty]$. When the parameter α satisfies the condition $0\prec\alpha\prec 1$, the function ϕ is concave. Then, according to the Jensen inequality, we can obtain:

$$\begin{aligned}\left(\sum_{\mathrm{k}=1}^{t}\frac{p_{\mathrm{k}}+q_{\mathrm{k}}}{2}\right)^{1-\alpha}&=\left(\sum_{\mathrm{k}=1}^{t}p_{\mathrm{k}}\frac{p_{\mathrm{k}}+q_{\mathrm{k}}}{2p_{\mathrm{k}}}\right)^{1-\alpha}\\&\ge\sum_{\mathrm{k}=1}^{t}p_{\mathrm{k}}\left(\frac{p_{\mathrm{k}}+q_{\mathrm{k}}}{2p_{\mathrm{k}}}\right)^{1-\alpha}\\&=\sum_{\mathrm{k}=1}^{t}p_{\mathrm{k}}^{\alpha}\left(\frac{p_{\mathrm{k}}+q_{\mathrm{k}}}{2}\right)^{1-\alpha}\end{aligned}$$

Because, $\sum_{\mathrm{k}=1}^{t}p_{\mathrm{k}}=\sum_{k=1}^{t}q_{\mathrm{k}}=1$, $\left(\sum_{k=1}^{t}(p_{\mathrm{k}}+q_{\mathrm{k}})/2\right)^{1-\alpha}=1$.

Therefore, it holds that $\sum_{\mathrm{k}=1}^{t}p_{\mathrm{k}}^{\alpha}\left((p_{\mathrm{k}}+q_{\mathrm{k}})/2\right)^{1-\alpha}\le 1$, and the equality holds if and only if $p_{\mathrm{k}}=q_{\mathrm{k}}$, $\forall$k.

Lemma 2: Let $A=(\mu_A,\nu_A)$ and $B=(\mu_B,\nu_B)$ be any two intuitionistic fuzzy numbers (IFNs). If f_I is a mapping, $f_I: IFN\times IFN\to[0,1]$. For $\alpha\in[0,1]$, then it holds:

$$\begin{aligned}\mathrm{f}_I(A,B)=&(\mu_A)^{\alpha}\left(\frac{\mu_A+\mu_B}{2}\right)^{1-\alpha}+(\nu_A)^{\alpha}\left(\frac{\nu_A+\nu_B}{2}\right)^{1-\alpha}\\&+(\pi_A)^{\alpha}\left(\frac{\pi_A+\pi_B}{2}\right)^{1-\alpha}\le 1\end{aligned} \tag{4}$$

where $\pi_A=1-\mu_A-\nu_A$, $\pi_B=1-\mu_B-\nu_B$

Proof of Lemma 2: Based on the definition of IFS, we obtain the following: $\mu_A+\nu_A+\pi_A=1$, and $\mu_B+\nu_B+\pi_B=1$, which imply that $(\mu_A+\mu_B)/2+(\nu_A+\nu_B)/2+(\pi_A+\pi_B)/2=1$.

Therefore, we conclude that $f_I(A,B)\le 1$ by Lemma 1, and the equality holds if and only if $A=B$, that is, $\mu_A=\mu_B$ and $\nu_A=\nu_B$.

Lemma 3: Let $A=\left(\left[\mu_A^L,\mu_A^H\right],\left[\nu_A^L,\nu_A^H\right]\right)$ and $B=\left(\left[\mu_B^L(\mathrm{x}_i),\mu_B^H\right],\left[\nu_B^L,\nu_B^H\right]\right)$ be any two IVIFNs. If f_{IV} is a mapping, $f_{IV}: IVIFN\times IVIFN\to[0,2]$. For $\alpha\in[0,1]$, then it holds:

$$\begin{aligned}&f_{IV}(A,B)\\&=\left(\mu_A^L\right)^{\alpha}\left(\frac{\mu_A^L+\mu_B^L}{2}\right)^{1-\alpha}+\left(\nu_A^L\right)^{\alpha}\left(\frac{\nu_A^L+\nu_B^L}{2}\right)^{1-\alpha}\\&\quad+\left(\pi_A^L\right)^{\alpha}\left(\frac{\pi_A^L+\pi_B^L}{2}\right)^{1-\alpha}+\left(\mu_A^H\right)^{\alpha}\left(\frac{\mu_A^H+\mu_B^H}{2}\right)^{1-\alpha}\\&\quad+\left(\nu_A^H\right)^{\alpha}\left(\frac{\nu_A^H+\nu_B^H}{2}\right)^{1-\alpha}+\left(\pi_A^H\right)^{\alpha}\left(\frac{\pi_A^H+\pi_B^H}{2}\right)^{1-\alpha}\\&\le 2.\end{aligned} \tag{5}$$

where $\pi_A=\left[\pi_A^L,\pi_A^H\right]=\left[1-\mu_A^H-\nu_A^H,1-\mu_A^L-\nu_A^L\right]$, $\pi_B=\left[\pi_B^L,\pi_B^H\right]=\left[1-\mu_B^H-\nu_B^H,1-\mu_B^L-\nu_B^L\right]$.

Proof of Lemma 3: Based on the definition of IVIFS, we obtain the following: $\mu_A^L+\nu_A^L+\pi_A^H=1$, $\mu_A^H+\nu_A^H+\pi_A^L=1$, $\mu_B^L+\nu_B^L+\pi_B^H=1$ and $\mu_B^H+\nu_B^H+\pi_B^L=1$, which imply that: $(\mu_A^L+\mu_B^L)/2+(\nu_A^L+\nu_B^L)/2+(\pi_A^H+\pi_B^H)/2=1$ and $(\mu_A^H+\mu_B^H)/2+(\nu_A^H+\nu_B^H)/2+(\pi_A^L+\pi_B^L)/2=1$.

Therefore, we conclude that $f_{IV}(A,B)\le 2$ by Lemma 2, and the equality holds if and only if $A=B$, that is, $\mu_A^L=\mu_B^L$, $\mu_A^H=\mu_B^H$, $\nu_A^L=\nu_B^L$, and $\nu_A^H=\nu_B^H$.

Now, we present the order-α divergence measure for IVIFNs.

Definition 5: Let $A=\left(\left[\mu_A^L,\mu_A^H\right],\left[\nu_A^L,\nu_A^H\right]\right)$ and $B=\left(\left[\mu_B^L(\mathrm{x}_i),\mu_B^H\right],\left[\nu_B^L,\nu_B^H\right]\right)$ be any two IVIFNs, and then we define the order-α divergence measure between two IVIFNs

A and B given by

$$D(\mathrm{A}\,|\mathrm{B}) = \frac{1}{\alpha-1}\left(\log_2\left(\begin{array}{l}(\mu_A^L)^\alpha\left(\frac{\mu_A^L+\mu_B^L}{2}\right)^{1-\alpha} \\ +(\mu_A^H)^\alpha\left(\frac{\mu_A^H+\mu_B^H}{2}\right)^{1-\alpha} \\ +(\nu_A^L)^\alpha\left(\frac{\nu_A^L+\nu_B^L}{2}\right)^{1-\alpha} \\ +(\nu_A^H)^\alpha\left(\frac{\nu_A^H+\nu_B^H}{2}\right)^{1-\alpha} \\ +(\pi_A^L)^\alpha\left(\frac{\pi_A^L+\pi_B^L}{2}\right)^{1-\alpha} \\ +(\pi_A^H)^\alpha\left(\frac{\pi_A^H+\pi_B^H}{2}\right)^{1-\alpha}\end{array}\right)-1\right) \tag{6}$$

To satisfy the symmetry of divergence measures, we define

$$D(\mathrm{A}\,\|\mathrm{B}) = {}^1\!/_2\,(D(\mathrm{A}\,|\mathrm{B}) + D(\mathrm{B}\,|A)) \tag{7}$$

as an order-α divergence measure for two IVIFNs A and B. Obviously, $D(\mathrm{A}\,\|\mathrm{B})$satisfies the properties DP1, DP2, and DP3.

Proof of Property DP1: We have $f_{IV}(A, B) \leq 2$ by Lemma 3. Then, for $\alpha \in [0, 1]$, we obtain $D(\mathrm{A}\,|\mathrm{B}) \geq 0$ and $D(\mathrm{B}\,|\mathrm{A}) \geq 0$. Therefore, it holds that $D(\mathrm{A}\,\|\mathrm{B}) \geq 0$, and the equality holds if and only if $A = B$.

Proof of Property DP2: When the distribution difference between A and B is the largest, their divergence value is also the largest. The maximum distribution difference between A and B has the following situations:

(1) $A = ([1, 1], [0, 0]), B = ([0, 0], [1, 1])$;
(2) $A = ([0, 0], [1, 1]), B = ([1, 1], [0, 0])$;
(3) $A = ([0, 0], [0, 0]), B = ([0, 0], [1, 1])$;
(4) $A = ([0, 0], [0, 0]), B = ([1, 1], [0, 0])$;
(5) $A = ([0, 0], [1, 1]), B = ([0, 0], [0, 0])$;
(6) $A = ([1, 1], [0, 0]), B = ([0, 0], [0, 0])$.

Their divergence values are also 1 in these cases by using (6) and (7). In other words, the maximum divergence is 1 between two IVIFNs A and B.

Therefore, $0 \leq D(\mathrm{A}\,\|\mathrm{B}) \leq 1$. *Property DP2* is established.

Property DP3 in fact holds when we define the order-α divergence measure for IVIFNs.

In summary, the order-α divergence measure in (7) is a standard divergence measure for IVIFNs.

Theorem 1: For all $A, B, W \in IVIFS$, the divergence measure$D(A\,\|B)$ satisfies the following properties:

(1) $D(\mathrm{A}\,\|\mathrm{A}\cup\mathrm{B}) = D(B\,\|A\cap\mathrm{B})$;
(2) $D(\mathrm{A}\,\|\mathrm{A}\cap\mathrm{B}) = D(B\,\|A\cup\mathrm{B})$;
(3) $D(\mathrm{A}\cup\mathrm{B}\,\|A\cap\mathrm{B}) = D(A\,\|B)$;
(4) $D(\mathrm{A}\,\|\mathrm{A}\cup B) + D(\mathrm{A}\,\|A\cap\mathrm{B}) = D(\mathrm{A}\,\|B)$;
(5) $D(\mathrm{A}\cup\mathrm{B}\,\|W) \leq D(\mathrm{A}\,\|W) + D(\mathrm{B}\,\|W)$;
(6) $D(\mathrm{A}\cap\mathrm{B}\,\|W) \leq D(\mathrm{A}\,\|W) + D(\mathrm{B}\,\|W)$;
(7) $D(\mathrm{A}\cup\mathrm{B}\,\|W) + D(\mathrm{A}\cap\mathrm{B}\,\|W) = D(\mathrm{A}\,\|W) + D(\mathrm{B}\,\|W)$;
(8) $D(\mathrm{A}\,\|\mathrm{B}) = D(\mathrm{A}^c\,\|\mathrm{B}^c)$; $D(\mathrm{A}\,\|\mathrm{B}^c) = D(A^c\,\|\mathrm{B})$;

Their proofs are straightforward by the operations and the definition of the order-α divergence measure for IVIFNs. Hence, we omit their proofs from here.

Now, we solve two examples in Table 1 again with our proposed measure, and the obtained divergence values are shown in Table 2.

TABLE 2. Divergence values with the proposed divergence measure.

α	A=([0.3,0.5],[0.3,0.5]), B=([0.2,0.3],[0.2,0.3])	A=([0.3,0.3],[0.6,0.6]), B=([0.2,0.2],[0.3,0.3])
0.1	0.081	0.017
0.2	0.087	0.034
0.3	0.092	0.050
0.4	0.098	0.065
0.5	0.104	0.081
0.6	0.109	0.095
0.7	0.115	0.109
0.8	0.121	0.123
0.9	0.127	0.136

The results presented in Table 2 clearly show that the divergence values are all not 0 by using the proposed divergence measure when A is not equal to B. Hence, the proposed measure is a valid and flexible divergence measure for IVIFNs, which can be employed to handle some problems related to various application fields.

IV. THE PROPOSED CRA APPROACH FOR ICSs

The framework of our proposed variable weight-based CRA approach for ICSs is shown in Fig. 2.

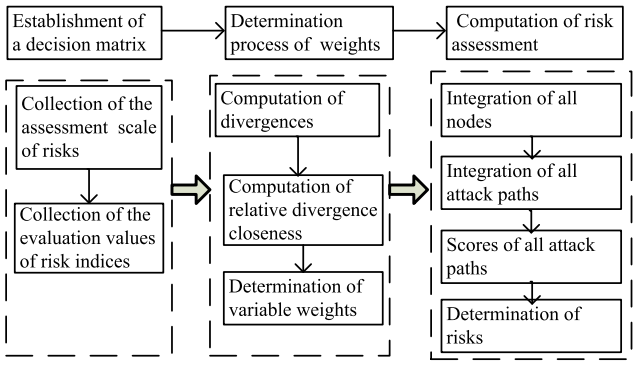

FIGURE 2. Framewor of ourvariable weight-based CRA approach.

The architecture of our approach consists of three main aspects: establishment of a decision matrix, determination of

variable weights, and risk assessment of ICSs. The establishment of a decision matrix includes the division of the risk level and the evaluation values of each attack accident given by experts. Evaluation values are expressed in the form of IVIFNs. The weights of risk indices are determined by the proposed divergence measure for IVIFNs. To ensure that the risks of ICSs can be better identified, the weights of risk indices are changed in the decision-making process, which is different from traditional CRA methods for ICSs. When the decision matrices and the weights of all attack accidents and defense strategies are obtained, all leaf nodes and each possible attack path can be integrated according to the operations for IVIFNs, and then, we can assess the highest risk with the score function of IVIFNs.

The implementation process of the CRA approach is shown in Table 3.

TABLE 3. The implementation process of the CRA approach.

Steps	Descriptions
Step 1	Determine the risk assessment scales of each index in the ICSs, and collect evaluation values of leaf nodes.
Step 2	Calculate the weights of risk indices for each leaf node based on the proposed divergence measure for IVIFNs.
Step 3	Integrate comprehensive values of all attack leaf nodes. Integrate comprehensive values of all defense nodes.
Step 4	Integrate comprehensive values of all attack paths.
Step 5	Calculate scores of all attack paths, and determine the most vulnerable links.

A. RISK ASSESSMENT SCALES

The risk assessment scales in this study are from [36]. We transform triangular fuzzy numbers (TFNs) into IVIFNs considering the same quantitative results. The quantization results of TFNs are calculated by the method in [67], in which the decision-maker's attitude is neutral. The scores of IVIFNs are calculated by using (2). The risk assessment scales in the form of IVIFNs are shown in Table 4.

B. DETERMINATION OF THE WEIGHTS

Since the maximum IVIFN is ([1, 1] , [0, 0]), the highest risk of leaf nodes A^+ in ICSs is defined as

$$A^+ = \{([1,1],[0,0]),([1,1],[0,0]),([1,1],[0,0])\}.$$

Since the minimum IVIFN is ([0, 0], [1, 1]), the lowest risk of leaf nodes A^-in ICSs is defined as

$$A^- = \{([0,0],[1,1]),([0,0],[1,1]),([0,0],[1,1])\}.$$

Next, we present the relative divergence closeness between the leaf nodes L_{ij} and the highest risk A^+ given by

$$\zeta_{ij} = \frac{D\left(L_{ij}\left\|A_j^+\right.\right)}{D\left(L_{ij}\left\|A_j^+\right.\right) + D\left(L_{ij}\left\|A_j^-\right.\right)} \tag{8}$$

where i is the number of leaf nodes and j is the number of risk indices.

The greater the relative divergence closeness is, the farther the leaf node is from the highest risk, and the smaller its weight should be. Conversely, the weight should be larger. The normalized weight of the leaf nodes L_{ij} is defined as

$$\omega_{ij} = \frac{1-\zeta_{ij}}{\mathrm{n} - \sum_{j=1}^{n}\zeta_{ij}} \tag{9}$$

where $\omega_{ij} \in [0,1]$, $\sum_{j=1}^{n}\omega_{ij} = 1$.

C. THE CALCULATION OF THE RISK ASSESSMENT

We define the integration expressions of attack leaf nodes, defense leaf nodes, combination nodes and attack paths in the ADT model based on the operations of IVIFNs.

1) INTEGRATION OF THE NODES

a: INTEGRATION OF ATTACK LEAF NODES

Suppose the evaluation values of the attack cost, attack difficulty and detection possibility for the ith attack leaf node are $\left(\left[\mu^L_{A_i,\cos t},\mu^H_{A_i,\cos t}\right],\left[\nu^L_{A_i,\cos t},\nu^H_{A_i,\cos t}\right]\right)$, $\left(\left[\mu^L_{A_i,diff},\mu^H_{A_i,diff}\right],\left[\nu^L_{A_i,\cos t},\nu^H_{A_i,diff}\right]\right)$ and $\left(\left[\mu^L_{A_i,\det},\mu^H_{A_i,\det}\right],\left[\nu^L_{A_i,\cos t},\nu^H_{A_i,\det}\right]\right)$, respectively, and its comprehensive evaluation value Z_{A_i} is defined as

$$\begin{aligned} Z_{A_i} &= \sum_{j=1}^{n}\omega_{A_i,j}r_{A_i,j} = \left(\left[\mu^L_{A_i},\mu^H_{A_i}\right],\left[\nu^L_{A_i},\nu^H_{A_i}\right]\right) \\ &= \left(\begin{bmatrix} 1-\left(1-\mu^L_{A_i,\cos t}\right)^{\omega_{A_i,\cos t}}\left(1-\mu^L_{A_i,diff}\right)^{\omega_{A_i,diff}} \\ \left(1-\mu^L_{A_i,\det}\right)^{\omega_{A_i,\det}}, \\ 1-\left(1-\mu^H_{A_i,\cos t}\right)^{\omega_{A_i,\cos t}}\left(1-\mu^H_{A_i,diff}\right)^{\omega_{A_i,diff}} \\ \left(1-\mu^H_{A_i,\det}\right)^{\omega_{A_i,\det}} \end{bmatrix}, \right. \\ &\quad \left. \begin{bmatrix} \left(\nu^L_{A_i,\cos t}\right)^{\omega_{A_i,\cos t}}\left(\nu^L_{A_i,diff}\right)^{\omega_{A_i,diff}} \\ \left(\nu^L_{A_i,\det}\right)^{\omega_{A_i,\det}}, \\ \left(\nu^H_{A_i,\cos t}\right)^{\omega_{A_i,\cos t}}\left(\nu^H_{A_i,diff}\right)^{\omega_{A_i,diff}} \\ \left(\nu^H_{A_i,\det}\right)^{\omega_{A_i,\det}} \end{bmatrix} \right) \end{aligned} \tag{10}$$

where $\omega_{A_i,\cos t}$, $\omega_{A_i,diff}$ and $\omega_{A_i,\det}$ represent the weight of the attack cost, attack difficulty and detection possibility for the ith attack leaf node, respectively, and

$$\omega_{A_i,\cos t} + \omega_{A_i,diff} + \omega_{A_i,\det} = 1.$$

b: INTEGRATION OF DEFENSE LEAF NODES

Suppose that the evaluation values of the defense cost, defense difficulty and defense time for the ith defense leaf node are $([\mu^L_{D_i,\cos t},\mu^H_{D_i,\cos t}],[\nu^L_{D_i,\cos t},\nu^H_{D_i,\cos t}])$, $([\mu^L_{D_i,diff},\mu^H_{D_i,diff}],[\nu^L_{D_i,diff},\nu^H_{D_i,diff}])$, and $([\mu^L_{D_i,time},\mu^H_{D_i,time}],[\nu^L_{D_i,time},\nu^H_{D_i,time}])$, respectively, then its comprehensive

TABLE 4. Risk assessment scales in the form of IVIFNs.

Attack cost	Evaluation values	Attack difficulty	Evaluation values	Detected possibility	Evaluation values
Very Low (VL)	([0.751,0.885], [0.001,0.115])	Very Low (VL)	([0.751,0.885], [0.001,0.115])	Very Low (VL)	([0.751,0.885], [0.001,0.115])
Low (L)	([0.558,0.659], [0.116,0.341])	Low (L)	([0.558,0.659], [0.116,0.341])	Low (L)	([0.558,0.659], [0.116,0.341])
Medium (M)	([0.500,0.500], [0.500,0.500])	Medium (M)	([0.500,0.500], [0.500,0.500])	Medium (M)	([0.500,0.500], [0.500,0.500])
High (H)	([0.116,0.341], [0.558,0.659])	High (H)	([0.116,0.341], [0.558,0.659])	High (H)	([0.116,0.341], [0.558,0.659])
Very High (VH)	([0.001,0.115], [0.751,0.885])	Very High (VH)	([0.001,0.115], [0.751,0.885])	Very High (VH)	([0.001,0.115], [0.751,0.885])

evaluation value Z_{D_i} is defined as

$$Z_{D_i} = \sum_{j=1}^{n} \omega_{D_i,j} r_{D_i,j} = \left(\left[\mu_{D_i}^L, \mu_{D_i}^H\right], \left[\nu_{D_i}^L, \nu_{D_i}^H\right]\right) = \left(\begin{bmatrix} 1-\left(1-\mu_{D_i,\cos t}^L\right)^{\omega_{D_i,\cos t}} \left(1-\mu_{D_i,diff}^L\right)^{\omega_{D_i,diff}} \\ \left(1-\mu_{D_i,time}^L\right)^{\omega_{D_i,time}} \end{bmatrix}, \begin{bmatrix} 1-\left(1-\mu_{D_i,\cos t}^H\right)^{\omega_{D_i,\cos t}} \left(1-\mu_{D_i,diff}^H\right)^{\omega_{D_i,diff}} \\ \left(1-\mu_{D_i,time}^H\right)^{\omega_{D_i,time}} \end{bmatrix}, \begin{bmatrix} \left(\nu_{D_i,\cos t}^L\right)^{\omega_{D_i,\cos t}} \left(\nu_{D_i,diff}^L\right)^{\omega_{D_i,diff}} \\ \left(\nu_{D_i,time}^L\right)^{\omega_{D_i,time}} \end{bmatrix}, \begin{bmatrix} \left(\nu_{D_i,\cos t}^H\right)^{\omega_{D_i,\cos t}} \left(\nu_{D_i,diff}^H\right)^{\omega_{D_i,diff}} \\ \left(\nu_{D_i,time}^H\right)^{\omega_{D_i,time}} \end{bmatrix}\right) \tag{11}$$

where $\omega_{D_i,\cos t}$, $\omega_{D_i,diff}$ and $\omega_{D_i,time}$ represent the weight of the defense cost, defense difficulty and defense time for the ith defense leaf node, respectively, and

$$\omega_{D_i,\cos t} + \omega_{D_i,diff} + \omega_{D_i,time} = 1.$$

c: INTEGRATION OF COMBINATION NODES

Let $Z_{A_i} = \left(\left[\mu_{A_i}^L, \mu_{A_i}^H\right], \left[\nu_{A_i}^L, \nu_{A_i}^H\right]\right)(i = 1, 2, \cdots, n)$ represent the comprehensive value of n attack leaf nodes, and then the integration value Z_i of the AND node is defined as

$$Z_i = Z_{A_1} \otimes Z_{A_2} \otimes \cdots \otimes Z_{A_n} = \left(\begin{bmatrix} \prod_{i=1}^{n} \mu_{A_i}^L, \prod_{i=1}^{n} \mu_{A_i}^H \end{bmatrix}, \begin{bmatrix} 1 - \prod_{i=1}^{n} \left(1-\nu_{A_i}^L\right), 1 - \prod_{i=1}^{n} \left(1-\nu_{A_i}^H\right) \end{bmatrix}\right) \tag{12}$$

The integration value of the OR node Z_i is defined as

$$Z_i = Z_{A_1} \cup Z_{A_2}, \cdots, \cup Z_{A_n} = \left(\begin{bmatrix} \max(\mu_{A_1}^L, \mu_{A_2}^L, \cdots, \mu_{A_n}^L), \\ \max(\mu_{A_1}^H, \mu_{A_2}^H, \cdots, \mu_{A_n}^H) \end{bmatrix}, \begin{bmatrix} \min(\nu_{A_1}^L, \nu_{A_2}^L, \cdots, \nu_{A_n}^L), \\ \min(\nu_{A_1}^H, \nu_{A_2}^H, \cdots, \nu_{A_n}^H) \end{bmatrix}\right). \tag{13}$$

d: THE OPERATION BETWEEN THE ATTACK NODES AND DEFENSE NODES

Let $Z_{A_i} = \left(\left[\mu_{A_i}^L, \mu_{A_i}^H\right], \left[\nu_{A_i}^L, \nu_{A_i}^H\right]\right)$ represent the comprehensive value of one attack leaf node, and let $Z_{D_i} = \left(\left[\mu_{D_i}^L, \mu_{D_i}^H\right], \left[\nu_{D_i}^L, \nu_{D_i}^H\right]\right)$ represent the comprehensive value of one defense leaf node. Therefore, the operation between the attack nodes and defense nodes is defined

$$R_i = Z_{A_i} \otimes Z_{D_i}^c = \left(\left[\mu_{A_i}^L, \mu_{A_i}^H\right], \left[\nu_{A_i}^L, \nu_{A_i}^H\right]\right) \otimes \left(\left[\nu_{D_i}^L, \nu_{D_i}^H\right], \left[\mu_{D_i}^L, \mu_{D_i}^H\right]\right) = \left(\begin{bmatrix} \mu_{A_i}^L \nu_{D_i}^L, \mu_{A_i}^H \nu_{D_i}^H \end{bmatrix}, \begin{bmatrix} 1-\left(1-\nu_{A_i}^L\right)\left(1-\mu_{D_i}^L\right), \\ 1-\left(1-\nu_{A_i}^H\right)\left(1-\mu_{D_i}^H\right) \end{bmatrix}\right) \tag{14}$$

2) INTEGRATION OF ATTACK PATHS

Assume that $X_{\text{path}} = \{X_1, X_2, \cdots, X_n\}$ is the attack path, where $X_t = \left(\left[\mu_t^L, \mu_t^H\right], \left[\nu_t^L, \nu_t^H\right]\right)(t = 1, 2, \cdots, m)$.

The comprehensive value of the attack path is expressed as

$$Z_{X_{\text{path}}} = X_1 \otimes X_2 \otimes \cdots \otimes X_m = \left(\begin{bmatrix} \prod_{t=1}^{m} \mu_t^L, \prod_{t=1}^{m} \mu_t^H \end{bmatrix}, \begin{bmatrix} 1 - \prod_{t=1}^{m} \left(1-\nu_t^L\right), 1 - \prod_{t=1}^{m} \left(1-\nu_t^H\right) \end{bmatrix}\right) \tag{15}$$

3) DETERMINATION OF RISK SCORES

Let $p = \left(\left[\mu_p^L, \mu_p^H\right], \left[\nu_p^L, \nu_p^H\right]\right)$ be the comprehensive value of any one attack path; and then the risk score of this attack

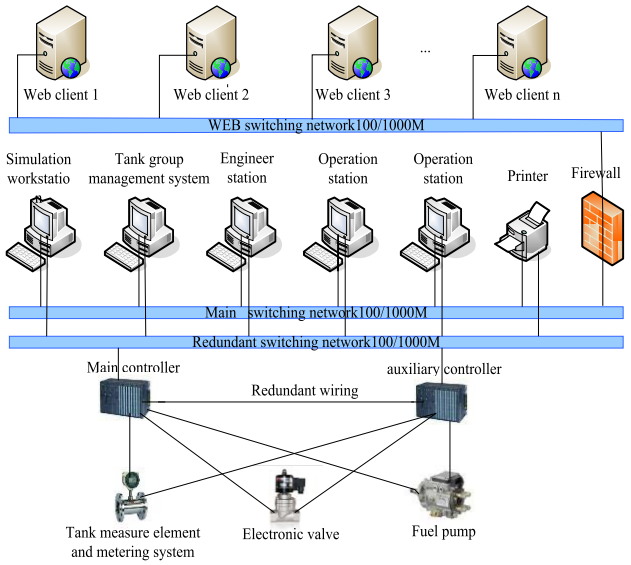

FIGURE 3. The network structure of an ICS for one civil aviation.

path is obtained by (12).

$$S(p) = \frac{1}{2}\left(\begin{array}{l}\mu_p^L + \mu_p^H + \dfrac{\mu_p^H + \nu_p^H}{2}\left(1 - \mu_p^L - \nu_p^L\right) \\ + \dfrac{\mu_p^L + \nu_p^L}{2}\left(1 - \mu_p^H - \nu_p^H\right)\end{array}\right) \tag{16}$$

V. APPLICATION AND ANALYSIS OF THE PROPOSED METHOD

A. APPLICATION

To demonstrate the application of the proposed cybersecurity risk assessment method, we consider the case discussed in [36]. The civil aviation fuel supply automatic control system is mainly divided into three logical levels: the enterprise management layer, process monitoring layer and field control layer. The network structure is shown in Fig. 3.

Fig. 4 is an ADT model against the civil aviation fuel supply automatic control system. The attack goal in the system is gaining access to the SCADA system. This is the root node in the ADT model. The possible risk events in the system include hardware failure, operator errors, Havex malware, Lnk file vulnerability, Printer Service Vulnerability, and MS08-067 vulnerability, which is to call the NetPathCanonicalize function in the server service program through the MSRPC over the SMB channel, causing the stack buffer to overflow to obtain Remote Code Execution, U disk injected with virus, Wincc vulnerability, Denial of service attack, replay attack and eavesdropping attack are the attack leaf nodes in the ADT model. The defense measure adopted in the system is to set up a firewall, which is the defense leaf node in the ADT model.

The CRA process of the proposed method for the system is shown in Fig. 5.

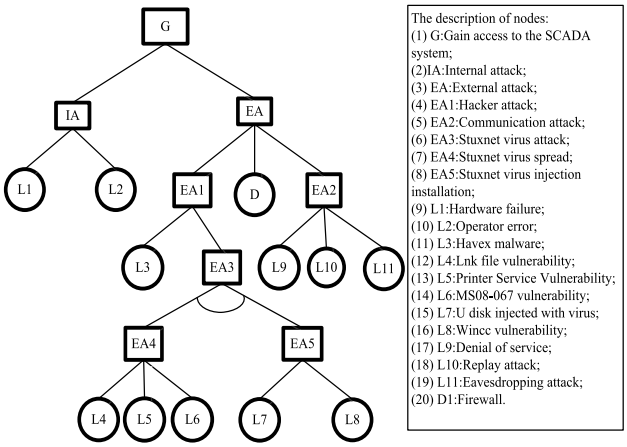

FIGURE 4. The ADT model of the automatic fuel supply control system.

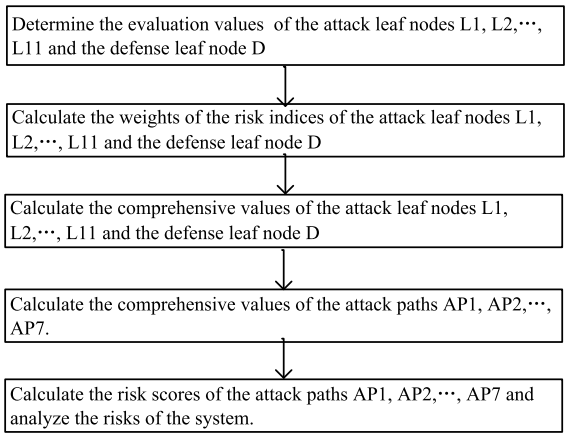

FIGURE 5. The CRAprocess of the proposed method for the system.

The calculation process of the cybersecurity risk assessment for the civil aviation fuel supply automatic control system is as follows:

Step 1: The evaluation values of attack leaf nodes and the defense leaf node are obtained by the method in Section 5.1, as shown in Table 5 and Table 6.

Step 2: The weights of all attack leaf nodes and the defense leaf node are obtained by the method in Section 4, respectively, as shown in Table 7 and Table 8 ($\alpha = 0.5$).

Step 3: Comprehensive values of all leaf nodes are calculated by using (10) and (11). The calculation results are shown in Table 9.

Step 4: Comprehensive values of each attack path are calculated by using (12), (13), (14), and (15). The results are shown in Table 10.

Step 5: Scores of all attack paths are obtained by using (16). The results are shown in Table 10.

Table 10 shows that the score of attack path AP2 is the highest, that is, the risk caused by operation error is the highest. The score of hardware failure is the second highest. The calculation results show that the key factor affecting the

TABLE 5. Evaluation values of attack leaf nodes.

Nodes	Attack Cost	Attack Difficulty	Detected Probability
L1	([0.751,0.885], [0.001,0.115])	([0.558,0.659], [0.116,0.341])	([0.500,0.500], [0.500,0.500])
L2	([0.751,0.885], [0.001,0.115])	([0.751,0.885], [0.001,0.115])	([0.116,0.341], [0.558,0.659])
L3	([0.116,0.341], [0.558,0.659])	([0.116,0.341], [0.558,0.659])	([0.558,0.659], [0.116,0.341])
L4	([0.558,0.659], [0.116,0.341])	([0.500,0.500], [0.500,0.500])	([0.558,0.659], [0.116,0.341])
L5	([0.500,0.500], [0.500,0.500])	([0.116,0.341], [0.558,0.659])	([0.558,0.659], [0.116,0.341])
L6	([0.558,0.659], [0.116,0.341])	([0.116,0.341], [0.558,0.659])	([0.558,0.659], [0.116,0.341])
L7	([0.751,0.885], [0.001,0.115])	([0.116,0.341], [0.558,0.659])	([0.558,0.659], [0.116,0.341])
L8	([0.558,0.659], [0.116,0.341])	([0.500,0.500], [0.500,0.500])	([0.500,0.500], [0.500,0.500])
L9	([0.001,0.115], [0.751,0.885])	([0.116,0.341], [0.558,0.659])	([0.500,0.500], [0.500,0.500])
L10	([0.558,0.659], [0.116,0.341])	([0.001,0.115], [0.751,0.885])	([0.116,0.341], [0.558,0.659])
L11	([0.558,0.659], [0.116,0.341])	([0.116,0.341], [0.558,0.659])	([0.558,0.659], [0.116,0.341])

TABLE 6. Evaluation values of the defense leaf node.

Nodes	Defense Cost	defense Difficulty	Detected Time
D1	([0.116,0.341], [0.558,0.659])	([0.116,0.341], [0.558,0.659])	([0.001,0.115], [0.751,0.885])

TABLE 7. The weights of attack leaf nodes.

Nodes	Attack Cost	Attack Difficulty	Detected Probability
L1	0.426	0.338	0.236
L2	0.432	0.432	0.136
L3	0.221	0.221	0.559
L4	0.371	0.259	0.371
L5	0.333	0.189	0.478
L6	0.418	0.164	0.418
L7	0.475	0.149	0.376
L8	0.418	0.291	0.291
L9	0.109	0.322	0.569
L10	0.654	0.088	0.258
L11	0.418	0.165	0.417

TABLE 8. The weights of defense leaf node.

Nodes	Defense Cost	Defense Difficulty	Detected Time
D1	0.427	0.427	0.145

securities of the civil aviation fuel supply automatic control system is internal security vulnerability. Measures should be strengthened in the training of personnel operation and maintenance of aircraft.

TABLE 9. Comprehensive values of leaf nodes.

Nodes	Comprehensive Values	Nodes	Comprehensive Values
L1	([0.644,0.7605], [0.022,0.235])	L7	([0.627,0.776], [0.015,0.225])
L2	([0.704,0.8854], [0.002,0.146])	L8	([0.525,0.574], [0.272,0.426])
L3	([0.400,0.544], [0.232,0.456])	L9	([0.352,0.418], [0.542,0.582])
L4	([0.544,0.624], [0.169,0.377])	L10	([0.432,0.560], [0.205,0.440])
L5	([0.475,0.561], [0.254,0.439])	L11	([0.505,0.620], [0.150,0.380])
L6	([0.505,0.620], [0.150,0.380])	D1	([0.100,0.312], [0.583,0.688])

TABLE 10. Comprehensive values of each attack path.

Attack Path	Attack Route	Comprehensive values	Scores
AP1	L1→IA	([0.453,0.654],[0.024,0.346])	0.684
AP2	L2→IA	([0.496,0.730],[0.005,0.270])	0.738
AP3	L3→EA1→EA	([0.047,0.126],[0.509,0.874])	0.198
AP4	EA3→EA1→EA	([0.040,0.112],[0.465,0.888])	0.200
AP5	L9→EA2→EA	([0.052,0.111],[0.702,0.890])	0.143
AP6	L10→EA2→EA	([0.064,0.148],[0.484,0.852])	0.219
AP7	L11→EA2→EA	([0.075,0.164],[0.448,0.836])	0.239

B. SENSITIVITY ANALYSIS OF THE PARAMETER

In what follows, the influence of different values of the parameter α on the risk ranking results of the system is discussed. The risk scores of all attack paths and the ranking results under different parameter α in the interval [0.1, 0.9] are shown in Table 11.

From Table 11, we notice that the risk scores of all attack paths increase with the increase of the parameterα. If the attitude toward the risk level is conservative, set the parameter $\alpha$to be small. If the attitude toward the risk levels is neutral, the parameterα is set to 0.5. If the attitude toward the risk levels is aggressive, the parameter α is set to be large. However, the risk ranking results varying with the parameter α are the same, and the attack paths of the highest risk are all AP2; that is, the changes in the parameter α do not have an effect on the risk ranking results, which indicates that the proposed order-α divergence measure for IVIFNs has good robustness.

C. COMPARISIONS AND DISCUSSION

To further prove the effectiveness of the proposed method in this paper, we still solve the CRA problem of the civil aviation fuel supply automatic control system by using these methods in [36], [45] and [61]. Triangular fuzzy numbers are adopted

TABLE 11. Ranking results under different parameter α.

α	Scores	Ranking
0.10	S(AP1)=0.682,S(AP2)=0.734,S(AP3) =0.194,S(AP4)=0.197,S(AP5)=0.140, S(AP6)=0.215,S(AP7)=0.236.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
0.20	S(AP1)=0.683,S(AP2)=0.736,S(AP3) =0.195,S(AP4)=0.198,S(AP5)=0.141, S(AP6)=0.216,S(AP7)=0.237.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
0.30	S(AP1)=0.684,S(AP2)=0.737,S(AP3) =0.196,S(AP4)=0.199,S(AP5)=0.142, S(AP6)=0.218,S(AP7)=0.238.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
0.40	S(AP1)=0.684,S(AP2)=0.737,S(AP3) =0.197,S(AP4)=0.199,S(AP5)=0.143, S(AP6)=0.219,S(AP7)=0.238.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
0.50	S(AP1)=0.684,S(AP2)=0.738,S(AP3) =0.198,S(AP4)=0.200,S(AP5)=0.143, S(AP6)=0.219,S(AP7)=0.239.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
0.60	S(AP1)=0.684,S(AP2)=0.738,S(AP3) =0.198,S(AP4)=0.200,S(AP5)=0.143, S(AP6)=0.220,S(AP7)=0.239.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
0.70	S(AP1)=0.684,S(AP2)=0.738,S(AP3) =0.198,S(AP4)=0.200,S(AP5)=0.143, S(AP6)=0.220,S(AP7)=0.239.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
0.80	S(AP1)=0.684,S(AP2)=0.738,S(AP3) =0.199,S(AP4)=0.201,S(AP5)=0.143, S(AP6)=0.220,S(AP7)=0.239.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
0.90	S(AP1)=0.684,S(AP2)=0.738,S(AP3) =0.199,S(AP4)=0.201,S(AP5)=0.143, S(AP6)=0.220,S(AP7)=0.239.	AP2>AP1>AP7> AP6>AP4>AP3> AP5

TABLE 12. Ranking results under different methods.

Methods	Scores	Ranking
the method in [36]	S(AP1)=0.752,S(AP2)=0.785, S(AP3)=0.562,S(AP4)=0.412, S(AP5)=0.436,S(AP6)=0.436, S(AP7)=0.561.	AP2>AP1>AP3> AP7>AP6=AP5> AP4
the method in [45] ($\gamma=-12.27$)	S(AP1)=0.685,S(AP2)=0.750, S(AP3)=0.126,S(AP4)=0.165, S(AP5)=0.103,S(AP6)=0.158, S(AP7)=0.198.	AP2>AP1>AP7> AP4>AP6>AP3> AP5
the method in [45] ($\gamma=0$)	S(AP1)=0.694,S(AP2)=0.726, S(AP3)=0.124,S(AP4)=0.164, S(AP5)=0.088,S(AP6)=0.170, S(AP7)=0.196.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
the method in [45] ($\gamma=8.60$)	S(AP1)=0.698,S(AP2)=0.709, S(AP3)=0.136,S(AP4)=0.190, S(AP5)=0.081,S(AP6)=0.183, S(AP7)=0.202.	AP2>AP1>AP7> AP4>AP6>AP3> AP5
the method in [61]	S(AP1)=0.605,S(AP2)=0.640, S(AP3)=0.155,S(AP4)=0.159, S(AP5)=0.113,S(AP6)=0.146, S(AP7)=0.202.	AP2>AP1>AP7> AP4>AP3>AP6> AP5
the method in this paper ($\alpha=0.15$)	S(AP1)=0.660,S(AP2)=0.702, S(AP3)=0.167,S(AP4)=0.177, S(AP5)=0.121,S(AP6)=0.179, S(AP7)=0.217.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
the method in this paper ($\alpha=0.55$)	S(AP1)=0.673,S(AP2)=0.717, S(AP3)=0.174,S(AP4)=0.183, S(AP5)=0.129,S(AP6)=0.193, S(AP7)=0.222.	AP2>AP1>AP7> AP6>AP4>AP3> AP5
the method in this paper ($\alpha=0.95$)	S(AP1)=0.679,S(AP2)=0.726, S(AP3)=0.181,S(AP4)=0.189, S(AP5)=0.134,S(AP6)=0.203, S(AP7)=0.227.	AP2>AP1>AP7> AP6>AP4>AP3> AP5

to describe evaluation values of risk indices and the weights of risk indices are determined by subjective weighting methods in [36]. IVIFNs are adopted to describe evaluation values of risk indices and the weights of risk indices are determined by the hybrid weighting method in [45]. IVIFNs are adopted to describe evaluation values of risk indices and the weights of risk indices are determined by the objective weighting method based on entropy in [61]. Among them, the weights of risk indices assigned by decision-makers are w=(0.500,0.333,0.167) in [36]. The range of the parameterγ is $-12.27 \leq \gamma \leq 8.60$ according to evaluation values of this example in [45]. The weights of risk indices obtained by using the entropy method are w=(0.287,0.340,0.373) in [61]. Ranking results under different methods are shown in Table 12.

Table 12 shows that the highest risk is all AP2 by using these methods. The ranking results in this paper are fully consistent with those in [45] ($\gamma = 0$) and almost identical to those in [45] ($\gamma = 12.87$ and $\gamma = 8.60$) and [61], except that the rankings of AP3, AP4 and AP6 are slightly different. The method in [36] cannot distinguish the risks of AP5 and AP6. Therefore, our proposed method is effective, and it can be used to handle the cybersecurity risk assessment problems of ICSs.

To further prove the advantages of the developed method in this paper, we give a counterexample to show that the ranking results of risks based on the existing approaches are unreasonable in some cases, while the proposed method can better identify risks.

TABLE 13. Evaluation values of Example 1.

Nodes	Attack Cost	Attack Difficulty	Detected Probability
L1	([0.001,0.115], [0.751,0.885])	([0.500,0.500], [0.500,0.500])	([0.751,0.885], [0.001,0.115])
L2	([0.751,0.885], [0.001,0.115])	([0.500,0.500], [0.500,0.500])	([0.116,0.341], [0.558,0.659])
L3	([0.500,0.500], [0.500,0.500])	([0.500,0.500], [0.500,0.500])	([0.500,0.500], [0.500,0.500])

Example 1: Suppose an expert evaluates the risk level of three attack leaf nodes (L1, L2, and L3) with regard to risk indices, including attack cost (G1), attack difficulty (G2) and detected probability (G3) in the form of IVIFNs, and their evaluation values are shown in Table 13.

We still utilize the above four methods to rank the risks, and the results are shown in Table 14. In this example, the range of the parameter γ is $-13.54 \leq \gamma \leq 11.21$ in [45].

From Table 14, we find that the highest risk is L1 by using the proposed method, and the ranking results of risks are the same as those in [61]. However, the highest risk is L2 by using the methods in [36] and [45]. Table 11 shows that for leaf node L1, the evaluation value of attack cost

TABLE 14. Ranking results under different methods of Example 1.

Methods	Weights	Scores	Ranking
the method in [36]	w11=w21=w31=0.500; w12=w22=w32=0.333; w13=w23=w33=0.167.	$S(A_1)$=0.528, $S(A_2)$=0.772, $S(A_3)$=0.500	$A_2>A_1>A_3$
the method in [45] ($\gamma=-13.54$)	w11=0.220,w12=0.706, w13=0.073;w21=0.264, w22=0.736,w23=0.000; w31=0.500,w32=0.333, w33=0.167.	$S(A_1)$=0.521, $S(A_2)$=0.702, $S(A_3)$=0.500	$A_2>A_1>A_3$
the method in [45] ($\gamma=0$)	w11=0.500,w12=0.333, w13=0.167;w21=0.500, w22=0.333,w23=0.167; w31=0.500,w32=0.333, w33=0.167.	$S(A_1)$=0.528, $S(A_2)$=0.772, $S(A_3)$=0.500	$A_2>A_1>A_3$
the method in [45] ($\gamma=11.21$)	w11=0.732,w12=0.024, w13=0.244;w21=0.695, w22=0.000,w23=0.305; w31=0.500,w32=0.333, w33=0.167.	$S(A_1)$=0.523, $S(A_2)$=0.809, $S(A_3)$=0.500	$A_2>A_1>A_3$
the method in [61]	w11=w21=w31=0.164; w12=w22=w32=0.557, w13=w23=w33=0.279	$S(A_1)$=0.679, $S(A_2)$=0.611, $S(A_3)$=0.500	$A_1>A_2>A_3$
the method in this paper ($\alpha=0.10$)	w11=0.213,w12=0.333, w13=0.454;w21=0.424, w22=0.311,w23=0.265; w31=0.333,w32=0.333, w33=0.334.	$S(A_1)$=0.741, $S(A_2)$=0.738, $S(A_3)$=0.500	$A_1>A_2>A_3$
the method in this paper ($\alpha=0.50$)	w11=0.132,w12=0.333, w13=0.535;w21=0.475, w22=0.295,w23=0.230; w31=0.333,w32=0.333, w33=0.334.	$S(A_1)$=0.778, $S(A_2)$=0.758, $S(A_3)$=0.500	$A_1>A_2>A_3$
the method in this paper ($\alpha=0.90$)	w11=0.094,w12=0.333, w13=0.573;w21=0.501, w22=0.292,w23=0.207; w31=0.333,w32=0.333, w33=0.334.	$S(A_1)$=0.793, $S(A_2)$=0.769, $S(A_3)$=0.500	$A_1>A_2>A_3$

is ([0.001,0.115],[0.751,0.885]), which is very small and far from the highest risk, while the evaluation value of the detected probability is ([0.751,0.885],[0.001,0.115]), which is very high and close to the highest risk. From the perspective of risk identification, the detected probability of leaf node L1 should be assigned a large weight, while the weight of attack cost should be assigned a small weight, so we allocate the weight of detected probability to 0.454 ($\alpha = 0.10$), 0.535 ($\alpha = 0.50$), and 0.573 ($\alpha = 0.90$). At the same time, we allocate the weight of attack cost to 0.213 ($\alpha = 0.10$), 0.132 ($\alpha = 0.50$), and 0.094 ($\alpha = 0.90$). However, the weight of attack cost assigned to all leaf nodes is always 0.500, and the weight of detected probability is always 0.167 in [36]. The weights of each index do not change with the evaluation information in the decision process; in that way, the identification of risks is easily confused when the evaluation of attack cost is relatively safe and the evaluation of detected probability is relatively dangerous. Although the weights of each index change with the evaluation information in the decision process in [45], the adjustments of weights depend on the discrimination between individual information and mean information with the parameter γ. As shown in Table 14, we find that the weight of attack cost is 0.220 ($\gamma = -13.54$), 0.500 ($\gamma = 0$), 0.732 ($\gamma = 11.21$), and the weight of detected probability is 0.073 ($\gamma = -13.54$), 0.167 ($\gamma = 0$), 0.244 ($\gamma = 11.21$) in the leaf node L1. The weights calculated by the method in [61] are 0.164, 0.557, and 0.279, respectively. Obviously, the assignment of weights is unreasonable and inconsistent with the actual situation in [36], [45] and [61]. Consequently, the proposed method fully considers the requirements of risk identification and can lead to a more reasonable risk assessment result.

Through the above discussion and analysis, we summarize the advantages of our methods compared with the other methods in detail below.

1. Different from traditional risk assessment methods, the weights of risk indices can be adjusted in the decision-making process by using our proposed method. They are determined by their closeness to the highest risk. Our proposed method can effectively recognize the highest risk because it fully considers the requirements of risk identification.
2. Our approach has good robustness and flexibility. Its ranking result of risks is stable and does not change with the change of the parameter α. In addition, decision-makers can also choose different values of the parameter α according to the different risk attitudes.

VI. CONCLUSION

In this paper, we define an order-α divergence measure for IVIFNs and develop a novel CRA method for ICSs under an interval-valued intuitionistic fuzzy environment. Finally, we apply the proposed method to the CRA of a civil aviation fuel supply automatic control system, verify its effectiveness and demonstrate its advantages.

In summary, our research has three main contributions: 1. We define an order-α divergence measure for IVIFNs, which can make up for the gap that there is no divergence measure with the parameter for IVIFNs. 2. We expand IVIFS to the CRA of ICSs and formulate integration approaches of all nodes and attack paths with IVIFNs in the ADT model. 3. We propose a novel CRA method for ICSs. In our method, we regard the weights of risk indices as variable weight vectors and develop a new technology to determine the weights of risk indices based on the proposed divergence measure. The proposed method can effectively avoid irrationality in the results of risk assessment compared with traditional CRA methods.

However, the proposed method also has its limitations: 1. It is only applicable to CRA problems in which evaluation values are expressed in the form of IVIFS. 2. The risk indices are regarded as independent without considering their mutual interaction in the integration process of leaf nodes.

In future research, we are committed to the following two aspects: 1. We will extend other fuzzy sets to the CRA of ICSs, for instance, interval-valued q-rung orthopair fuzzy sets. 2. We will advance some novel CRA methods for ICSs considering the interactions among risk indices.

REFERENCES

[1] 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.

[2] A. W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, "Industrial cyberphysical systems: A backbone of the fourth industrial revolution," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 6–16, Mar. 2017.

[3] C. Zhou, B. Hu, Y. Shi, Y.-C. Tian, X. Li, and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proc. IEEE*, vol. 109, no. 4, pp. 517–541, Apr. 2021.

[4] M. D. Firoozjaei, N. Mahmoudyar, Y. Baseri, and A. A. Ghorbani, "An evaluation framework for industrial control system cyber incidents," *Int. J. Crit. Infrastruct. Protection*, vol. 36, Mar. 2022, Art. no. 100487.

[5] R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102376.

[6] M. Iaiani, A. Tugnoli, S. Bonvicini, and V. Cozzani, "Analysis of cybersecurity-related incidents in the process industry," *Rel. Eng. Syst. Saf.*, vol. 209, May 2021, Art. no. 107485.

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

[8] X. Li, C. Zhou, Y.-C. Tian, N. Xiong, and Y. Qin, "Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 608–618, Feb. 2018.

[9] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43586–43601, 2018.

[10] J. Wang, M. Neil, and N. Fenton, "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101659.

[11] 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.

[12] Y. Sun, K. Hou, H. Jia, J. Rim, D. Wang, Y. Mu, X. Yu, and L. Zhu, "An incremental-variable-based state enumeration method for power system operational risk assessment considering safety margin," *IEEE Access*, vol. 8, pp. 18693–18702, 2020.

[13] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Saf. Sci.*, vol. 131, Nov. 2020, Art. no. 104908.

[14] C.-H. Chang, C. Kontovas, Q. Yu, and Z. Yang, "Risk assessment of the operations of maritime autonomous surface ships," *Rel. Eng. Syst. Saf.*, vol. 207, Mar. 2021, Art. no. 107324.

[15] A. V. Jha, B. Appasani, A. N. Ghazali, and N. Bizon, "A comprehensive risk assessment framework for synchrophasor communication networks in a smart grid cyber physical system with a case study," *Energies*, vol. 14, no. 12, p. 3428, Jun. 2021.

[16] B. Cabezali and F. Santos, "Application of a fuzzy-logic based model for risk assessment in additive manufacturing R&D projects," *Comput. Ind. Eng.*, vol. 145, Jul. 2020, Art. no. 106529.

[17] X. Gou, Z. Xu, W. Zhou, and E. Herrera-Viedma, "The risk assessment of construction project investment based on prospect theory with linguistic preference orderings," *Econ. Res.-Ekonomska Istraživanja*, vol. 34, no. 1, pp. 709–731, Jan. 2021.

[18] X. Wang, X. Gou, and Z. Xu, "Assessment of traffic congestion with ORESTE method under double hierarchy hesitant fuzzy linguistic environment," *Appl. Soft Comput.*, vol. 86, Jan. 2020, Art. no. 105864.

[19] S. Tabatabaee, A. Mahdiyar, and S. Ismail, "Towards the success of building information modelling implementation: A fuzzy-based MCDM risk assessment tool," *J. Building Eng.*, vol. 43, Nov. 2021, Art. no. 103117.

[20] K. Kaewfak, V.-N. Huynh, V. Ammarapala, and N. Ratisoontorn, "A risk analysis based on a two-stage model of fuzzy AHP-DEA for multimodal freight transportation systems," *IEEE Access*, vol. 8, pp. 153756–153773, 2020.

[21] 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, Mar. 2019, 3574675.

[22] A. A. Tubis, S. Werbińska-Wojciechowska, M. Góralczyk, A. Wróblewski, and B. Ziętek, "Cyber-attacks risk analysis method for different levels of automation of mining processes in mines based on fuzzy theory use," *Sensors*, vol. 20, no. 24, p. 7210, Dec. 2020.

[23] Z. Huang, T. Le, Y. Gao, X. Yao, H. Wang, W. Zhao, Y. Zhang, and N. Nie, "Safety assessment of emergency training for industrial accident scenarios based on analytic hierarchy process and gray-fuzzy comprehensive assessment," *IEEE Access*, vol. 8, pp. 144767–144777, 2020.

[24] S. Xie, S. Dong, Y. Chen, Y. Peng, and X. Li, "A novel risk evaluation method for fire and explosion accidents in oil depots using bow-tie analysis and risk matrix analysis method based on cloud model theory," *Rel. Eng. Syst. Saf.*, vol. 215, Nov. 2021, Art. no. 107791.

[25] 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.

[26] M. Gul, B. Guven, and A. F. Guneri, "A new Fine–Kinney-based risk assessment framework using FAHP-FVIKOR incorporation," *J. Loss Prevention Process Ind.*, vol. 53, pp. 3–16, May 2018.

[27] M. Gul and E. Celik, "Fuzzy rule-based Fine–Kinney risk assessment approach for rail transportation systems," *Hum. Ecol. Risk Assessment: Int. J.*, vol. 24, no. 7, pp. 1786–1812, 2018.

[28] W. Wang, X. Liu, X. Chen, and Y. Qin, "Risk assessment based on hybrid FMEA framework by considering decision maker's psychological behavior character," *Comput. Ind. Eng.*, vol. 136, pp. 516–527, Oct. 2019.

[29] X.-Y. Li, Z.-L. Wang, Y. Xiong, and H.-C. Liu, "A novel failure mode and effect analysis approach integrating probabilistic linguistic term sets and fuzzy Petri nets," *IEEE Access*, vol. 7, pp. 54918–54928, 2019.

[30] C. Zhou, X. Li, S. Yang, and Y.-C. Tian, "Risk-based scheduling of security tasks in industrial control systems with consideration of safety," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3112–3123, May 2020.

[31] Y. Jianxing, C. Haicheng, W. Shibo, and F. Haizhao, "A novel risk matrix approach based on cloud model for risk assessment under uncertainty," *IEEE Access*, vol. 9, pp. 27884–27896, 2021.

[32] J. Mi, W. Huang, M. Chen, and W. Zhang, "A method of entropy weight quantitative risk assessment for the safety and security integration of a typical industrial control system," *IEEE Access*, vol. 9, pp. 90919–90932, 2021.

[33] D. Tian, Y. Wang, and T. Yu, "Fuzzy risk assessment based on interval numbers and assessment distributions," *Int. J. Fuzzy Syst.*, vol. 22, no. 4, pp. 1142–1157, Jun. 2020.

[34] D. K. Jana and R. Ghosh, "Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security," *J. Inf. Secur. Appl.*, vol. 40, pp. 173–182, Jun. 2018.

[35] M. Abbaspour Onari, S. Yousefi, and M. Jahangoshai Rezaee, "Risk assessment in discrete production processes considering uncertainty and reliability: Z-number multi-stage fuzzy cognitive map with fuzzy learning algorithm," *Artif. Intell. Rev.*, vol. 54, no. 2, pp. 1349–1383, Feb. 2021.

[36] S. Wang, L. Ding, H. Sui, and Z. Gu, "Cybersecurity risk assessment method of ICS based on attack-defense tree model," *J. Intell. Fuzzy Syst.*, vol. 40, no. 6, pp. 10475–10488, 2021.

[37] P. A. G. Aguirre, L. Perez-Dominguez, D. Luviano-Cruz, E. M. Gomez, I. J. C. P. Olguin, and J. O. D. Ramirez, "Risk assessment with value added Pythagorean fuzzy failure mode and effect analysis for stakeholders," *IEEE Access*, vol. 9, pp. 149560–149568, 2021.

[38] M. Akram, A. Luqman, and J. C. R. Alcantud, "Risk evaluation in failure modes and effects analysis: Hybrid TOPSIS and ELECTRE i solutions with Pythagorean fuzzy information," *Neural Comput. Appl.*, vol. 33, no. 11, pp. 5675–5703, Jun. 2021.

[39] A. Karasan, E. Ilbahar, S. Cebi, and C. Kahraman, "A new risk assessment approach: Safety and critical effect analysis (SCEA) and its extension with Pythagorean fuzzy sets," *Saf. Sci.*, vol. 108, pp. 173–187, Oct. 2018.

[40] L. Wang and H. Garg, "Algorithm for multiple attribute decision-making with interactive Archimedean norm operations under Pythagorean fuzzy uncertainty," *Int. J. Comput. Intell. Syst.*, vol. 14, no. 1, pp. 503–527, 2021.

[41] K. Atanassov and G. Gargov, "Interval-valued intuitionistic fuzzy sets," *Fuzzy Sets Syst.*, vol. 31, pp. 343–349, Jan. 1989.

[42] K. Atanassov, "Operators over interval valued intuitionistic fuzzy sets," *Fuzzy Sets Syst.*, vol. 64, no. 2, pp. 159–174, Jun. 1994.

[43] Z. S. Xu, "Methods for aggregating interval-valued intuitionistic fuzzy information and their application to decision making," *J. Control Decis.*, vol. 22, no. 2, pp. 215–220, Feb. 2007.

[44] X. Gou, Z. Xu, and H. Liao, "Exponential operations of interval-valued intuitionistic fuzzy numbers," *Int. J. Mach. Learn. Cybern.*, vol. 7, no. 3, pp. 501–518, Jun. 2016.

[45] S. Liu, W. Yu, F. T. S. Chan, and B. Niu, "A variable weight-based hybrid approach for multi-attribute group decision making under interval-valued intuitionistic fuzzy sets," *Int. J. Intell. Syst.*, vol. 36, pp. 1015–1052, Nov. 2020.
[46] H. Garg and K. Kumar, "A novel exponential distance and its based TOPSIS method for interval-valued intuitionistic fuzzy sets using connection number of SPA theory," *Artif. Intell. Rev.*, vol. 53, no. 1, pp. 595–624, Jan. 2020.
[47] K. Kumar and S.-M. Chen, "Multiattribute decision making based on interval-valued intuitionistic fuzzy values, score function of connection numbers, and the set pair analysis theory," *Inf. Sci.*, vol. 551, pp. 100–112, Apr. 2021.
[48] R. Che, C. Suo, and Y. Li, "An approach to construct entropies on interval-valued intuitionistic fuzzy sets by their distance functions," *Soft Comput.*, vol. 25, no. 10, pp. 6879–6889, May 2021.
[49] W. Zhou, J. Chen, B. Ding, and S. Meng, "Interval-valued intuitionistic fuzzy envelopment analysis and preference fusion," *Comput. Ind. Eng.*, vol. 142, Apr. 2020, Art. no. 106361.
[50] H. Bustince, C. Marco-Detchart, J. Fernandez, C. Wagner, J. M. Garibaldi, and Z. Takáć, "Similarity between interval-valued fuzzy sets taking into account the width of the intervals and admissible orders," *Fuzzy Sets Syst.*, vol. 390, pp. 23–47, Jul. 2020.
[51] K. Deveci, R. Cin, and A. Kağizman, "A modified interval valued intuitionistic fuzzy CODAS method and its application to multi-criteria selection among renewable energy alternatives in Turkey," *Appl. Soft Comput.*, vol. 96, Nov. 2020, Art. no. 106660.
[52] D. Bhandari and N. R. Pal, "Some new information measures for fuzzy sets," *Inf. Sci.*, vol. 67, no. 3, pp. 209–228, Jan. 1993.
[53] J. Ye, "Fuzzy cross entropy of interval-valued intuitionistic fuzzy sets and its optimal decision-making method based on the weights of alternatives," *Expert Syst. Appl.*, vol. 38, no. 5, pp. 6179–6183, May 2011.
[54] F. Meng and J. Tang, "Interval-valued intuitionistic fuzzy multiattribute group decision making based on cross entropy measure and choquet integral," *Int. J. Intell. Syst.*, vol. 28, no. 12, pp. 1172–1195, Dec. 2013.
[55] X. Qi, C. Liang, and J. Zhang, "Generalized cross-entropy based group decision making with unknown expert and attribute weights under interval-valued intuitionistic fuzzy environment," *Comput. Ind. Eng.*, vol. 79, pp. 52–64, Jan. 2015.
[56] F. Meng and X. Chen, "Interval-valued intuitionistic fuzzy multi-criteria group decision making based on cross entropy and 2-additive measures," *Soft Comput.*, vol. 19, no. 7, pp. 2071–2082, Jul. 2015.
[57] I. Montes, N. R. Pal, V. Janis, and S. Montes, "Divergence measures for intuitionistic fuzzy sets," *IEEE Trans. Fuzzy Syst.*, vol. 23, no. 2, pp. 444–456, Apr. 2015.
[58] F. Wang and S. Wan, "Possibility degree and divergence degree based method for interval-valued intuitionistic fuzzy multi-attribute group decision making," *Expert Syst. Appl.*, vol. 141, Mar. 2020, Art. no. 112929.
[59] Y. H. Li, Y. Cheng, Q. Mou, and S. Xian, "Novel cross-entropy based on multi-attribute group decision-making with unknown experts' weights under interval-valued intuitionistic fuzzy environment," *Int. J. Comput. Intell. Syst.*, vol. 13, no. 1, pp. 1295–1304, 2020.
[60] A. R. Mishra, A. Chandel, and D. Motwani, "Extended MABAC method based on divergence measures for multi-criteria assessment of programming language with interval-valued intuitionistic fuzzy sets," *Granular Comput.*, vol. 5, no. 1, pp. 97–117, Jan. 2020.
[61] A. R. Mishra, P. Rani, K. R. Pardasani, A. Mardani, Ž. Stević, and D. Pamučar, "A novel entropy and divergence measures with multi-criteria service quality assessment using interval-valued intuitionistic fuzzy TODIM method," *Soft Comput.*, vol. 24, no. 15, pp. 11641–11661, Aug. 2020.
[62] Y. Song, Q. Fu, Y. Wang, and X. Wang, "Divergence-based cross entropy and uncertainty measures of Atanassov's intuitionistic fuzzy sets with their application in decision making," *Appl. Soft Comput.*, vol. 84, Nov. 2019, Art. no. 105703.
[63] R. Verma, "On intuitionistic fuzzy order-α divergence and entropy measures with MABAC method for multiple attribute group decision-making," *J. Intell. Fuzzy Syst.*, vol. 40, no. 1, pp. 1191–1217, 2021.
[64] B. Schneier, "Attack trees," *Dr. Dobb's J.*, vol. 24, no. 12, pp. 21–29, 1999.
[65] B. Kordy, S. Mauw, S. Radomirovic, and P. Schweitzer, "Attack-defense trees," *J. Log. Comput.*, vol. 24, no. 1, pp. 55–87, Feb. 2014.
[66] R. P. Yao, "An approach to variable weight group decision-making based on improved scoring function of interval intuitionistic fuzzy sets," *Stat. Decis.*, vol. 34, no. 11, pp. 36–38, 2019.
[67] T.-S. Liou and M.-J.-J. Wang, "Ranking fuzzy numbers with integral value," *Fuzzy Sets Syst.*, vol. 50, no. 3, pp. 247–255, Sep. 1992.

HUIJUAN GUO received the Ph.D. degree from the School of Electrical Engineering, Hebei University of Technology, Tianjin, China, in 2013. She is currently a Lecturer at the School of Information Engineering, Tianjin University of Commerce, Tianjin. Her current research interests include security assessments of industrial control systems and fuzzy decision analysis.

LEI DING received the M.S. degree in computer technology from the Civil Aviation University of China, China. He is currently working as an Engineer at the Information Center of the Civil Aviation Administration of China. His current research interests include the Internet of Things, industrial control systems, network security, and vulnerability analysis.

WENCHAO XU received the M.S. degree from the Hebei University of Technology, Tianjin, China, in 2009. He is currently a Lecturer at the School of Information Engineering, Tianjin University of Commerce, Tianjin. His research interests include pattern recognition, intelligent control, and deep learning.