

Received June 4, 2021, accepted June 16, 2021, date of publication June 21, 2021, date of current version July 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3091136

A Method of Entropy Weight Quantitative Risk Assessment for the Safety and Security Integration of a Typical Industrial Control System

JUNPENG MI¹, WENJUN HUANG¹, MENGCHI CHEN¹, AND WEI ZHANG²

¹Department of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China

²Department of Industrial Communication Technology, Zhejiang Supcon Technology Company Ltd., Hangzhou 310053, China

Corresponding author: Wenjun Huang (wjhuang@iipc.zju.edu.cn)

This work was supported by the Chinese Key Research and Development Program under Project 2018YFB1700101.

ABSTRACT Aiming at the risk assessment requirements of typical industrial control systems with integrated architecture of security and safety, we propose an objective and quantitative integrated security and safety assessment scheme based on Fuzzy Analytic Hierarchy Process (FAHP). First, we establish a safety and security integrated (SSI) architecture for typical industrial control systems with security measures integrated into safety failure modes. On this basis, we establish a hierarchical model of risk assessment with SSI failure mode as an element of the evaluation layer, and then standardize characteristic values of various safety-related heterogeneous index parameters. We design an entropy weight method that uses Grey Relation Analysis (GRA) method to modify the correlation of multiple indicators as a parameter strategy for determining the relative importance of element layer and evaluation layer and then use the membership function method of fuzzy statistical method to obtain the membership degree of hierarchical elements, and finally obtain the failure risk level value of equipment and system by fuzzy comprehensive evaluation. Based on a typical distributed control system, we build an experimental platform to test and verify the risk assessment plan, and compared with expert experience parameter method. The result shows that the scheme takes into account the correlation between indicators which measure the SSI risk level of industrial control system, and the entropy weight method is used to evaluate the risk of industrial control system which can overcome the subjectivity and uncertainty of individual judgment. Furthermore, the quantitative evaluation of system risk is completed by using fuzzy statistical method in the case of industrial control system without prior knowledge, and the idea of this scheme has a wide range of engineering value.

INDEX TERMS Security and safety integrated, fuzzy analytic hierarchy process, failure mode, risk assessment, grey relation analysis.


I. INTRODUCTION

With the application and integration of network architecture of smart factories, safety-related equipment does not exist in the form of independent isolation, but needs to be interconnected.

For the safety of industrial control system, security protection requirements are necessary regarding how to balance and coordinate the resolution of contradiction between safety and

security, IEC standard only provides the trade-off principle, that is, the implementation of security should not affect safety. There is no recognized solution in the industry.

Domestic and foreign solutions for the integration of safety and security can be roughly divided into two parts: unified and integrated methods [1]. The unified method can be summarized as constructing a unified risk and vulnerability analysis framework for security and security according to specific requirements and corresponding standards [2]–[5], and designing a step-by-step process for risk and vulnerability analysis covering safety integration accordingly.

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Khurram Khan .

The integration scheme is mainly to integrate safety and security into different stages of the system development life cycle [6]–[8]. Eames and Moffet [9] proposed an integrated method of applying safety and security risk analysis processes to determine the integration requirements. By comparing the requirements in the safety documents with security model, the two safety requirements were analyzed and identified, the interaction between and vice versa. These general methods often deal with safety and security in the concept and requirements stage. For existing systems, in order to identify possible interactions, model-based methods are more suitable. Woskowski [10] proposed a risk-based approach to improve the safety and security of critical medical devices by extending risk management required by IEC14971 beyond device boundaries; the objective is to cover interface safety, interface usage and network security aspects, as well as to define security related hazardous situations in the risk estimation phase. Schmittner *et al.* [11] described an approach for combine analysis of safety and security in which the basic failure mode and effect analysis (FMEA) of cause and effect is extended to include security related aspects.

For industrial control system risk assessment methods, the typical method is to use the fault tree analysis method, such as Ralston [12], [13] discussed the quantitative analysis method of attack probability based on fault tree to evaluate the security of SCADA system. This method clearly shows the attack process and mechanism and the disadvantage is that most of the fault mechanisms in practice are fuzzy, not a simple 0-1 relationship, and it is easy to misdiagnose using accurate fault cause data for analysis. Bayesian networks based on the integration of probability theory and graph theory are used for security assessment. Xin *et al.* [14] proposed an information security risk assessment method based on fuzzy theory and Bayesian regularized BP neural network for the large amount of ambiguity and over-fitting in the process of security risk assessment. The determination of conditional probability of the Bayesian network model is generally more complicated, and it is often determined by expert experience or statistical experiment based on specific problems. Shang *et al.* [15] proposed a security risk assessment method based on the attack tree model, which combines fuzzy theory and probabilistic risk assessment technology. The disadvantage is that only static evaluation methods are used to evaluate and analyze attacks, and there is a lack of research on dynamic methods. The above methods have two main deficiencies: one is how to accurately analyze each security attribute; the other is how to quantitatively analyze the occurrence probability of each leaf node to reduce the influence of subjective factors. Tay and Lim [16] introduced fuzzy logic method into FMEA and proposed a rule simplification scheme to determine fuzzy priority, which greatly simplified the complexity of risk assessment process. In order to improve the effectiveness of FMEA, Song *et al.* [17] obtained a more reasonable failure mode ranking based on rough set theory. Rafie and Namin [18] used FMEA and fuzzy inference system (FIS) to predict subsidence risk. Fuzzy theory is able to simulate

uncertainty. Compared with traditional FMEA, it can work in a better way under the condition of fuzzy concept and insufficient information. However, for safety and security which have different rules and need to be integrated, the limitations of fuzzy FMEA are highlighted under the condition of multi-level and multi object of industrial control system. In recent years, many researchers have begun to apply Analytic Hierarchy Process (AHP) to the security modeling and risk assessment of industrial control systems. For example, Leau *et al.* [19] used the AHP_FCE comprehensive method to evaluate security from three aspects: risk factors, service factors, and public factors. Hassan *et al.* [20] used risk analysis method FMEA combined with fuzzy-AHP to identify and reduce the possible process failures in warehousing. These methods are qualitative and quantitative decision-making methods that can achieve complex goals, but its analysis results are highly subjective, and the risk assessment results include personal factors.

In recent years, the integration of safety and security in industrial control field has become a research hotspot. Many experts and scholars have formulated a variety of excellent SSI model schemes and corresponding risk assessment algorithms based on the IEC international standard regulations and the characteristics of industrial control systems, and continue to promote the research process of integration of safety and security, but these methods also have some problems:

1. The analytic hierarchy process and other quantitative methods in the process of risk assessment of industrial control system security are seriously subjective in parameter weight assignment, especially when the possibility of industrial control system equipment being attacked is converted into the relative weight assignment of system equipment, it is generally determined by the decision maker directly designates, and the designation process relies on the personal preference and experience of the expert.

2. In the process of hierarchical modeling, due to the complexity of the working conditions of industrial control systems, the elements in each level are not completely unrelated, and there is a lack of correlation analysis of the elements in the scheme layer of the model during the process of risk assessment.

This paper builds a safety and security integrated industrial control system architecture that integrates security measures into safety failure modes. Based on the establishment of a hierarchical model of risk assessment with safety integrated failure modes as an element of the evaluation layer, we design a weight vector decision-making scheme optimized by entropy weight and use the GRA method to complete the correlation analysis between failure modes. We take the multi-index entropy weight method instead of the expert weight method as a parameter strategy for determining the relative importance of element layer and evaluation layer and construct a membership function by the fuzzy statistical method to obtain the membership degree of the layer elements, and then the risk assessment value of equipment and system are obtained through the fuzzy comprehensive

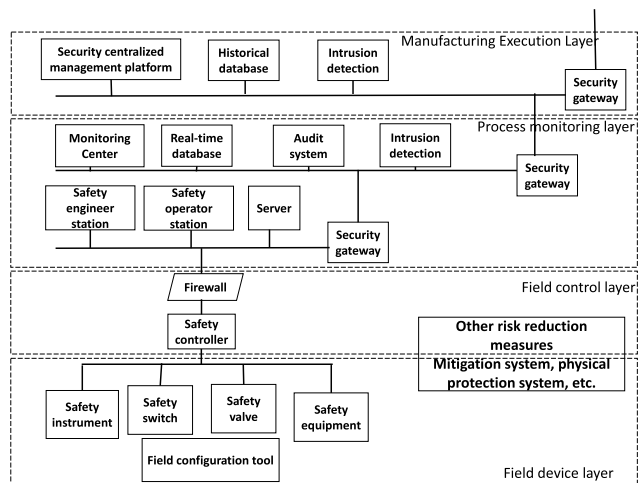


FIGURE 1. The network structure of a typical SSI system application in the process industry.

evaluation. For the risk assessment of industrial control system without prior knowledge of risk, this method can carry out effective and quantitative risk assessment according to the system’s own risk related operating condition and has wide application value.

II. METHODS

A. SSI ARCHITECTURE

1) PRINCIPLES OF COLLABORATIVE DESIGN OF SSI SYSTEM

The SSI system is a system that integrates safety control, security protection and intelligent safety management to realize the risk control requirements of smart factories.

- Field device layer, generally includes: field safety instruments, field safety transmitters, field safety execution equipment, network equipment (under fieldbus architecture), etc.
- Field control layer, generally including: safety control equipment, network equipment, industrial firewall, etc.
- Process monitoring layer, generally including: security engineer station, security operator station, server, database, monitoring center, network equipment, security gateway, intrusion detection system, etc.
- Manufacturing execution layer, generally including: security centralized management platform, database, security gateway, etc.

This paper does not make specific requirements for the selection of functional safety equipment or the selection of information security equipment, because there are complete functional safety related standards for the process industry or offline industry, such as: GB/T21109.1, GB28526, GB/T16855.1, and the requirements of security related equipment can also refer to IEC 62443-4-2. According to the requirements of IEC 62859 Nuclear Power Plant-Instrumentation and Control System-Coordination of Safety and Network Security, in its 5.2 section, there is a provision that the implementation of security should not affect safety, and this

TABLE 1. Principles of system collaborative design.

| No | Object | Subject | Principles |
|----|-----------------------|--|---|
| 1 | Safety | Implementation of security measures | Modify unacceptable subject |
| 2 | Safety | Invalidation of security measures | Capable of leading to a safety state |
| 3 | Security requirements | Avoidance of negative effects on safety | Appropriate alternative measures (compensation measures) should be adopted to reduce the risk to a tolerable range |
| 4 | Design of Safety | Realization of necessary security requirements | Object should be fully demonstrated |
| 5 | Safety | Security measures | Subject should be developed and evaluated in accordance with the reliability, availability, maintainability, and quality objectives required |
| 6 | Safety | Security measures | Subject need to be integrated with safety-related systems and fully tested before the system is put into operation to ensure that object of the system will not cause unacceptable negative effects |

provision is used as the design principle of SSI system, that is, the system collaborative design principle is to ensure that there is no conflict between safety and security.

Although we have put forward the requirements of system which needs collaborative design, there are various specific implementation methods in different industrial environments. For example, the authentication technology can use static passwords, smart cards, SMS verification codes, biometric technology, etc. Means, for different applications, it is necessary to specifically consider what measures are appropriate, which will not affect the safety of system. At the same time, the reliability and stability of the selected equipment also need to be ensured by on-site testing.

2) COLLABORATIVE DESIGN SCHEME OF SSI SYSTEM

The integration of safety and security of industrial control systems and equipment can seek a trade-off between each other from the perspectives of multiple dimensions and multiple indicators. Considering that safety is the foundation of industrial control equipment/systems, the key safety elements of the system operation process include task instructions, function parameters, maximum response time of functions and maximum utilization of resources. Security protection measures may affect one or more aspects of these elements. The most important principle is that security protection measures should not prevent the system from meeting its required

functions and performance. This paper aims to ensure the normal operation of equipment/systems (safety) as the goal. By using security protection measures as threat sources that affect safety measures and using FMEA technology to complete the traversal analysis of security-related measures on safety to achieve the impact analysis between security protection measures. And then we complete the consequence analysis of using security-related measures as the failure mode, and determine the implementation of security-oriented control strategies.

TABLE 2. Dimensions of technical requirements for security protection.

| GB/T 33009.1 | GB/T 33008.1 | GB/T T21109.1 | IEC 62443-3-3 | This paper |
|-----------------------------------|-----------------------------------|-------------------------------------|-----------------------------------|-----------------------------------|
| Area division | Use control | Use control | Use control | Area division |
| Access control | System integrity | Resource control | System integrity | Access and use control |
| Intrusion prevention | Data confidentiality | Data security | Data confidentiality | Data security |
| Identification and authentication | Identification and authentication | Identification and authentication | Identification and authentication | Identification and authentication |
| Security audit | Restricted data flow | Security audit | Restricted data flow | Intrusion prevention |
| Resource control | Timely response to incidents | Area division and Border protection | Timely response to incidents | Resource control |

For the requirements of security measures, as shown in Table 2, it shows the dimensional requirements of security technologies under various standards. Among them, IEC 62443 Security of Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels from several dimensions of identification and authentication control, usage control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability put forward requirements for the security protection design of industrial automation and control systems. Although the dimensions described by the standards are slightly different, the essential core ideas are the same, that is, the requirements for availability, integrity, and confidentiality are required.

This paper regards the dimensions of regional division, identification and authentication, access and use control, resource control, data security, intrusion prevention, and security auditing as the key elements of security protection technical requirements.

According to the possible negative effects of relevant security protection measures on safety, the security requirements are divided into two levels: basic requirements and enhanced requirements. The basic requirements are the general basic design requirements, that is, the level 2 goal of safety perfection is expected to be achieved; the strengthening requirements are the design requirements added to the basic requirements, that is, the level 1 goal of safety perfection is expected to be achieved. The security protection design of the safety and security integrated system should at least achieve the specified basic requirements, and systems with high security protection requirements can choose to implement the

Algorithm 1 SSI Process

Input: Security measures for designated function blocks
 Output: Design scheme under SSI risk requirements

- 1: s_0 // Definition of safety measure s_0
- 2: s_L // Safety requirement level
- 3: t_0 // Pre-adopt security measure t_0
- 4: t_L // Security requirement level
- 5: $t_0(F)$ // Failure of pre-adopted security measures t_0
- 6: m_0 // reliability, availability and other safety performance requirements
- 7: if $m_0(s_0 \cup t_0(F)) < m_0(s_0)$ then
- 8: if $t_L(s_0 \cup t_0(F)) < t_L(s_0)$ then
- 9: $t_0 \leftarrow t_0 \cup t_{0s}$ / t_{0s} is the compensation measure of t_0
- 10: if $t_L(s_0 \cup t_0(F)) \geq t_L(s_0)$ then
- 11: $t_0 \leftarrow t_{00}$ //Choose application scheme t_{00} from application scope to application method
- 12: $P(t_{00})$ // Risk assessment to determine feasible solutions
- 13: end if
- 14: end if
- 15: end if
- 16: return $P(t_{00})$

specified enhanced requirements. According to the collaborative design principles analyzed in the previous section, the design of the collaborative scheme is completed.

3) OVERVIEW OF SSI SYSTEM

Our goals in designing this system are:

- 1) Based on the premise that security measures should not affect the safety function of industrial control system/equipment, a system architecture integrating safety and security is designed.
- 2) Based on the SSI design criteria, we construct a hierarchical model of SSI, and design a risk level scheme that can objectively and quantitatively describe the SSI system.

We next discuss the details of the proposed system architecture (shown in Figure 2):

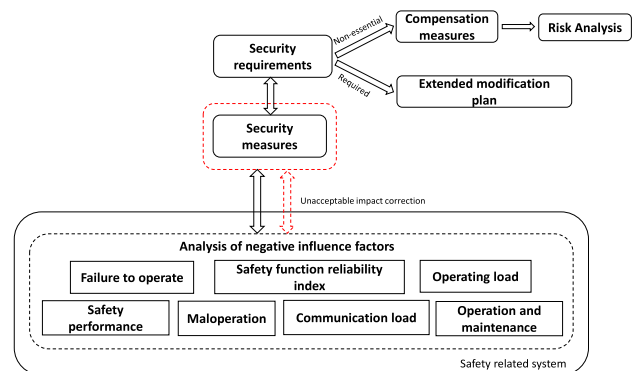


FIGURE 2. SSI system architecture.

- The security protection measures for unacceptable negative effects of the system should be modified (the dotted

line indicates the failure of information security protection measures). The most relevant factors for security functions are given in this paper and the negative responses include the elements those shown in the figure but not limited to them;

- The effectiveness of the security protection measures (for example: communication security) on which any security function depends should be monitored. If any failure is found, an alarm should be issued in time to support the user in targeted processing. The design plan should be able to ensure that the failure will not affect the execution of the safety function;
- The feasible design changes are as follows.: if the result is an increase in the frequency of the requirements of the safety function, the requirement mode of the safety function can be redefined, and the safety-related system can be redesigned and evaluated. If the result affects the safety integrity of the safety function itself, for example, after the security protection measures are added to the safety circuit, if the PFD/PFH parameters of safety circuit do not meet the SIL target, new safety functions can be added to meet the overall safety requirements of the system.

B. SSI RISK ASSESSMENT MODELING

The risk assessment scheme designed in this paper is shown in the figure 3. Details will be expanded in sections.

1) RISK ASSESSMENT HIERARCHICAL MODEL

Considering that the security protection and intrusion prevention requirements of an SSI system can reflect the conflicts and connections between security and security in various security indicators, taking the possible attack and defense situations in the communication process as an example, security attack events are composed of threat sources, attack paths, and vulnerable target objects of initiated events. Safety incidents are generally caused by faults or design flaws of industrial control equipment/systems. In the proposed industrial control system environment, identify the possible consequences when a safety event occurs in the equipment/system, and based on the consequences, identify the security attack events that will lead to these consequences as the focus of risk assessment. This paper takes this as the research focus, combined with the standard IEC 61784 communication security layer for the safety failure modes that may appear in the data communication process, and design the impact analysis of SSI failure based on the same failure result, as shown in Table 3:

The industrial control system is a system with complex levels and high dimensions. Fuzzy analytic hierarchy process can effectively process fuzzy evaluation objects through accurate digital means, and can make a more scientific, reasonable, and practical quantitative evaluation to the fuzzy data in the hidden information. The safety of the entire system is constrained by a variety of technical requirements. The risk assessment of the system identifies assets from two aspects:

TABLE 3. Impact analysis of SSI failure.

| Failure mode | Safety measures | Security measures | The impact of security measures |
|---|-----------------------------------|---|---|
| Corruption of messages (safety) | Discard error messages | Detect error data based on traffic characteristics or protocol analysis | False detection or missed detection interferes with communication quality |
| Data tampering (security) | | | |
| Accidental repetition (safety) | Discard error messages | SYN Cookie mechanism | The pressure on the security firewall increases and quality decreases |
| Out of order (safety) | | | |
| Flooding attack (security) | | | |
| Message camouflage (safety) | Discard error messages | Add new secure communication channel | The risk of other attacks increases |
| Message insertion (safety) | | | |
| MITM attack (security) | | | |
| Mis operation by unauthorized personnel (safety) | Discard error messages | Identity management and data encryption | The real-time quality increases |
| Insider attack (security) | | | |
| Unacceptable delay (safety) | Time out to enter fail-safe state | Analyze the cause of delay and response | The quality of safety decreases and risk increases |
| Most cyber-attacks (security) | | | |

meeting SSI requirements and process requirements, forming asset class elements. Identify system vulnerabilities according to the severity of asset vulnerabilities elements and then comprehensively identify SSI failure modes and the deployed safety measures faced by industrial control systems.

For the risk assessment of industrial control SSI systems, the analysis process is similar to the security assessment. We divide the risk assessment model of industrial control systems into three levels: the target layer, which is the risk assessment value of the industrial control system or equipment; the criterion layer, which is the dimension of the security protection technology requirements and the measured indicator dimensions of the SSI system designed in this paper (analog “assets”); the solution layer, that is, the possible failure modes of SSI (analog “vulnerability”), as shown in Figure 4.

We further analyze the risk assessment model of industrial control systems. Taking a typical industrial control system or equipment as an example, the target layer of the analytic hierarchy model is the risk assessment value of the industrial

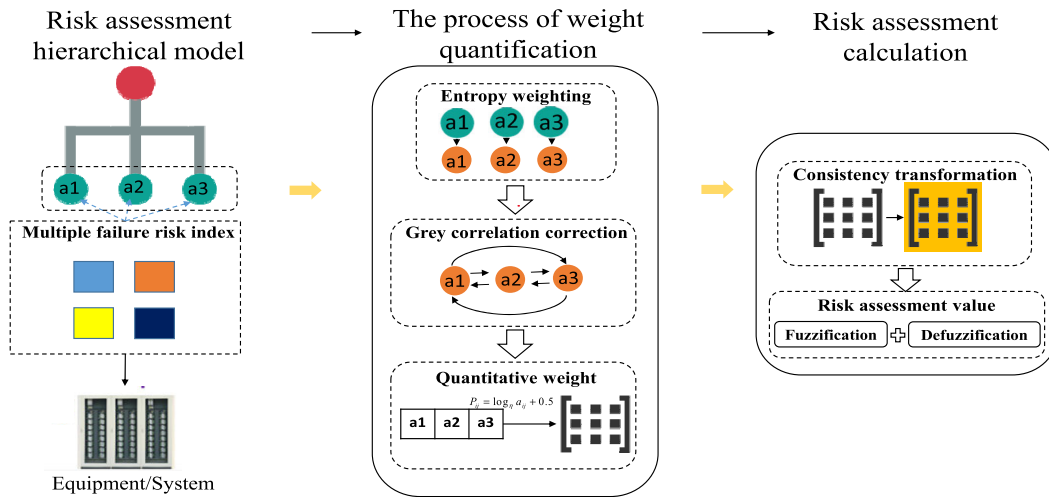


FIGURE 3. SSI system risk assessment scheme.

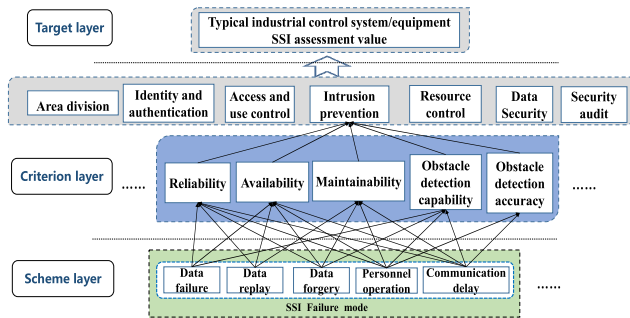


FIGURE 4. Hierarchical risk assessment model of SSI.

control system or equipment in Figure 3; The second criterion layer includes seven dimensions of security protection technology requirements for SSI systems, that is, area division, identity and authentication, access and use control, intrusion prevention, resource control, data security and security audit. Taking intrusion prevention requirements as an example, we use five risk indicators including reliability, availability, maintainability, obstacle detection capability, and obstacle detection accuracy to measure it. At the scheme layer, five failure modes of SSI are used as optional solutions for security risk assessment as evaluation indicators, which are communication data failure, data replay, data forgery, personnel operation, and communication delay. In Figure 3, the arrow points from the failure mode to the five indicators, which means that the failure mode will have a negative impact on the pointed indicator, and the arrow points from the indicator to the technical requirements, indicating that the level of technical requirements is determined by the indicator at the front of the arrow. We focus on intrusion prevention requirements and several indicators representing its SSI attributes are mainly affected by the five failure modes in Figure 3, but this cannot replace the evaluation criteria for risk levels of other technical requirements, and needs to be analyzed separately.

2) MULTI-INDEX ENTROPY WEIGHTING

The fuzzy analytic hierarchy process mainly includes four steps: the establishment of hierarchical structure model, the construction of judgment matrix, the consistency check, the fuzzification and the de-fuzzification [21]. After completing the level analysis modeling, we determine the relative importance of each factor at this level according to the relative degree of influence of each factor on the level above. In order to quantitatively describe the relative importance, we give a quantitative scale of 0.1 to 0.9. Considering the differences in risk assessment standards under different process environments of industrial control SSI systems, we design a quantitative scale method that can be dynamically defined.

Let $P_{ij} = \log_{\eta} a_{ij} + 0.5$, then

$$P_{ij}(\eta) = P_{ik}(\eta) - P_{jk}(\eta) + 0.5 \quad (1)$$

Equation (1) shows that the scale order can be kept unchanged under the fuzzy consistency conversion, and the redefining scale method is given and the comparison between element A_i and element A_j is shown in Table 4.

The particularity of each element of each layer makes the upper element corresponding to each element be affected to different degrees, and the degree of interrelation between elements of each layer is not the same. It is necessary to seek a judgment scheme that can quantify these relationships to make a quantitative risk assessment of the system. First, we analyze the possible impact of the five SSI failure modes at the scheme layer on the criterion layer indicators after threats, and make weight decisions to determine the relative importance of the five SSI failure modes, and construct a judgment matrix. We take DCS as an example to assign importance by completing failure consequence analysis. Taking into account the pursuit of the highest availability and real-time performance in DCS communication process, that is, the protection of safety cannot be at the cost of obstructing the normal production process. As shown in Table 5, we use

TABLE 4. Quantitative scaling method of priority relation judgment matrix.

| Scaling | Meaning |
|--|--|
| 0.5 | equally important |
| $\log_{\eta} 3 + 0.5$ | A_i is slightly more important than A_j |
| $\log_{\eta} 5 + 0.5$ | A_i is obviously more important than A_j |
| $\log_{\eta} 7 + 0.5$ | A_i is strongly important than A_j |
| $\log_{\eta} 9 + 0.5$ | A_i is extremely important than A_j |
| $\log_{\eta} i + 0.5 \quad i = 2, 4, 6, 8$ | the scale when the two adjacent scales are compromised |
| Complementary scales listed above | If the element A_i is compared with the element A_j and the judgment r_{ij} is obtained, then the element A_j and the element A_i are compared with the judgment $r_{ji} = 1 - r_{ij}$ |

TABLE 5. Correspondence between failure modes and process indicators.

| Failure mode Evaluation index | Data failure | Data replay | Data forgery | Personnel operation | Communication delay |
|---|--------------|-------------|--------------|---------------------|---------------------|
| Reliability (mean time before failure(s)) | A_1 | A_2 | A_3 | A_4 | A_5 |
| Availability (mean time between failures (s)) | B_1 | B_2 | B_3 | B_4 | B_5 |
| Maintainability (average time before recovery(s)) | C_1 | C_2 | C_3 | C_4 | C_5 |
| Obstacle detection capability (failure detection rate (%)) | D_1 | D_2 | D_3 | D_4 | D_5 |
| Obstacle detection accuracy (false alarm rate (%)) | E_1 | E_2 | E_3 | E_4 | E_5 |

time domain indicators such as the reliability, availability, and maintainability (RAM) of DCS as well as the fault detection rate and false alarm rate as parameters determining risk level. We count the process data of various indicators and measure the relative importance of elements by the measured values of objective indicators to avoid randomness and subjectivity caused by subjective preferences of subjective weighting methods such as expert experience method.

There is a causal relationship among the five SSI failure modes given in Table 5 and the communication delay is almost the failure effect caused by all failure modes. We use the GRA method to quantitatively analyze the correlation between other failure modes and communication delay.

We first conduct a qualitative analysis of various failure modes, and give a causal pair,

$$CE = \{(x, y) | x, y \in \{A, B, C, D, E\}, x \neq y\}, \quad y \rightarrow x \quad (2)$$

For $(x_0, y_i) \in (x_0, y)$, where $x_0 = (x_{01}, x_{02}, \dots, x_{0q}) \in x$, $y_i = (y_{i1}, y_{i2}, \dots, y_{iq})$, we normalize y_i and calculate the deviation between y_i and x_0 . Then, we determine the correlation

coefficient ε_{0i} under the optimal index sequence with x_0 , and the deviation Δ_{ij} is defined as,

$$\Delta_{ij} = |y_{ij} - x_{0j}|, \quad \Delta_{\min} = \min_i \min_j \Delta_{ij},$$

$$\Delta_{\max} = \max_i \max_j \Delta_{ij} \quad 1 \leq i \leq p, \quad 1 \leq j \leq q \quad (3)$$

Therefore, the GRA coefficient between the j -th index of the i -th ‘‘cause’’ object and the j -th index of the ‘‘effect’’ object in the causality pair is:

$$\varepsilon_{ij} = \frac{\Delta_{\min} + \rho \Delta_{\max}}{\Delta_{ij} + \rho \Delta_{\max}}, \quad 1 \leq i \leq p, \quad 1 \leq j \leq q \quad (4)$$

Only from the safety attributes of the indicators themselves, we quantify the relative importance of safety process indicators by analyzing the information entropy value. According to the definition of information entropy, for a certain index, the entropy value can be used to judge the degree of dispersion of an index. The smaller the entropy value, the greater the degree of dispersion of the index, and the greater the influence of the index on the comprehensive evaluation (that is, the weight).

In the bid evaluation problem with m evaluation index and n bidding scheme (hereinafter referred to as (m, n) bid evaluation problem), the entropy of the i evaluation index is defined as,

$$H_i = -k \sum_{j=1}^n f_{ij} \ln f_{ij}, \quad i = 1, 2, \dots, m \quad (5)$$

where

$$f_{ij} = \frac{x_{ij}}{\sum_{j=1}^n x_{ij}}, \quad k = \frac{1}{\ln n} \quad (6)$$

And suppose that when $f_{ij} = 0, f_{ij} \ln f_{ij} = 0$.

In bid evaluation problem (m, n) , the entropy weight of the i -th indicator is defined as:

$$\omega_i = \frac{1 - H_i}{m - \sum_{i=1}^m H_i} \quad (7)$$

Based on the above theories, we propose a GRA method for optimizing entropy weights, and design a multi-index dynamic weight decision scheme based on the relative importance of elements in fuzzy analytic hierarchy:

(a) Assuming that an index system is composed of m indicators to evaluate n failure modes, the eigenvalue of the i index of the j failure mode is x_{ij} , and the eigenvalue matrix of the indicators can be obtained as follows:

$$X = (x_{ij})_{m \times n} \quad (8)$$

For a given i, x_{ij} , the greater the difference between them, the greater the relative strength of the index value between different failure modes, the more information it carries and transmits, and the greater the threat to the system.

(b) We standardize the eigenvalues, and obtain the standardized eigenvalue matrix: $X' = (x'_{ij})_{m \times n}$. The purpose is to

eliminate the difficulty in comparison between the indicators due to different dimensions. In the evaluation indicators, there are usually benefits, cost and fixed indicators. The standardization methods for various indicators are given below:

Let $H_i = -k \sum_{j=1}^n f_{ij} \ln f_{ij}$, $i = 1, 2, \dots, m$, where T_i represents the benefit-type, cost-type, and fixed-type subscript sets respectively; α_i represents the best stable value of the fixed-type indicator.

$$y_{ij} = \frac{x_{ij} - \min_j x_{ij}}{\max_j x_{ij} - \min_j x_{ij}} \quad j \in [1, n] i \in T_1 \quad (9)$$

$$y_{ij} = \frac{\max_j x_{ij} - x_{ij}}{\max_j x_{ij} - \min_j x_{ij}} \quad j \in [1, n] i \in T_2 \quad (10)$$

$$y_{ij} = 1 - \frac{|x_{ij} - \alpha_i|}{\max_j |x_{ij} - \alpha_i|} \quad j \in [1, n] i \in T_3 \quad (11)$$

(c) Determine the entropy weight of each index according to formulas (5) and (6). It can be seen from formula (5) that when $x_{i1} = x_{i2} = \dots = x_{in}$, $H_i = H_{\max} = \ln n$, then the indicators have no effect on the comparison of various failure modes and can be deleted from the index system. When i is fixed and j takes a different value, the greater the difference between the value of y_{ij} , the more information the indicator transmits, the greater the effect, and the greater its weight.

(d) The quantitative value of the relative importance of failure modes is determined by the objective weight of each index—the GRA coefficient ε_{ij} between the entropy weight and the failure mode. The failure mode q is selected as the causal pair of the “effect” object, and the importance weight is

$$V_q = \sum_{i=1}^m \omega_{iq} x'_{iq} - \sum_{j=1}^n \sum_{i=1}^m \varepsilon_{ij} \omega_{ij} x'_{ij} + \sum_{i=1}^m \varepsilon_{iq} \omega_{iq} x'_{iq} \quad (12)$$

$$RI = \{r_q | r_q = \frac{V_q}{\sum_{q=1}^n V_q}\} \quad (q = 1, 2, \dots, n) \quad (13)$$

where ω_{ij} is the entropy weight value of the i -th evaluation index of the j -th failure mode, x'_{ij} is the index value after standardization, and RI is the set of the importance weights of various failure modes.

3) SSI RISK LEVEL VALUE CALCULATION

We use entropy optimization method to quantify and determine the relative importance of each failure mode, as shown in Table 6,

Therefore, the judgment matrix R_{DCS} is,

$$R_{DCS} = \begin{bmatrix} 0.5 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ 1 - \alpha_1 & 0.5 & \beta_1 & \beta_2 & \beta_3 \\ 1 - \alpha_2 & 1 - \beta_1 & 0.5 & \chi_1 & \chi_2 \\ 1 - \alpha_3 & 1 - \beta_2 & 1 - \chi_1 & 0.5 & \delta_1 \\ 1 - \alpha_4 & 1 - \beta_3 & 1 - \chi_2 & 1 - \delta_1 & 0.5 \end{bmatrix} \quad (14)$$

TABLE 6. The relative importance of failure modes.

| DCS | Data failure | Data replay | Data forgery | Personnel operation | Communication delay |
|---------------------|----------------|---------------|--------------|---------------------|---------------------|
| Data failure | 0.5 | α_1 | α_2 | α_3 | α_4 |
| Data replay | $1 - \alpha_1$ | 0.5 | β_1 | β_2 | β_3 |
| Data forgery | $1 - \alpha_2$ | $1 - \beta_1$ | 0.5 | χ_1 | χ_2 |
| Personnel operation | $1 - \alpha_3$ | $1 - \beta_2$ | $1 - \chi_1$ | 0.5 | δ_1 |
| Communication delay | $1 - \alpha_4$ | $1 - \beta_3$ | $1 - \chi_2$ | $1 - \delta_1$ | 0.5 |

We complete the normalization process for RI . Because of $A_n, B_n, C_n, D_n \in (0, 1)$, we use equation (15) to complete the mapping between the weight and the relative importance value domain,

$$X_n = \begin{cases} \frac{m}{2}, & m \in (0, 1) \\ \frac{m - 0.5}{m}, & m \in [1, +\infty) \end{cases} \quad (15)$$

m is the normalized importance weight. After consistency conversion according to formula (17), the fuzzy consistency judgment matrix $R = (f_{ij})_{n \times n}$ is obtained.

$$r_i = \sum_{k=1}^n r_{ik} \quad (16)$$

$$f_{ij} = \frac{r_i - r_j}{2n} + 0.5 \quad (17)$$

After transforming the judgment matrix R_{DCS} into a fuzzy consensus matrix R_{CDCS} according to formula (17), and calculating the SSI attribute weight of each failure mode in the scheme layer to DCS according to formula (18),

$$\omega_i = \frac{1}{n} - \frac{1}{2\alpha} + \frac{1}{n\alpha} \times \sum_{j=1}^n f_{ij} \quad (18)$$

α is inversely proportional to the difference of weights, that is, the larger α , the smaller the difference of weights; the smaller α , the greater the difference of weights. When $\alpha = (n - 1)/2$, the difference in weight is the largest. In this paper, we take $\alpha = 2$ and R_{CDCS} is a 5th-order matrix. The weight vectors of the 5 evaluation indexes of DCS can be obtained,

$$W_{DCS} = [\omega_1, \omega_2, \omega_3, \omega_4, \omega_5] \quad (19)$$

A unified set of comments is used to judge each element, making the results more comparable. According to the SSI assessment model of industrial control systems shown in Figure 3, the five failure mode indicators in the scheme layer of the hierarchical model are fuzzy evaluated.

The fuzziness and certainty of the SSI evaluation index can be transformed, that is, its fuzziness can be transformed into a certain degree of membership relative to the quality level. We use the completed SSI system quantification priority relationship judgment matrix quantitative scale criteria in Table 4,

and re-quantitatively rank the qualitative relationships such as “slightly” and “obvious” with the numerical relationship of the SSI indicators under DCS.

We set up a fuzzy comment set and divide the comment set into 5 levels, that is, the comment set $E = \{\text{very safe, relatively safe, basic safe, relatively dangerous, very dangerous}\}$, and the rating value of the comment is based on the quantitative relationship in Table 4.

According to formula (20), we obtain the fuzzy risk rating result of each failure mode on the DCS.

$$V_i = W_i E_i \tag{20}$$

We use the fuzzy statistical method to obtain the system reliability, availability, maintainability and other indicators from the process measurement data, and arrange the level of indicator data according to the level of the comment level. According to the proportion of the data set obtained by classification, the membership degrees of the five failure modes are calculated. And then get the fuzzy SSI rating result V_{DCS} of the DCS.

The evaluation result V_{DCS} obtained by fuzzy comprehensive evaluation is a fuzzy vector. In order to make the result of the system risk assessment more obvious, the fuzzy vector of the comprehensive evaluation result is de-fuzzified. We use the following formula to de-fuzzify the final fuzzy vector:

$$V'_{DCS} = \frac{\sum_{j=1}^n f_{vj} v_j}{\sum_{j=1}^n f_{vj}} \tag{21}$$

According to formula (21), the final SSI risk level value of DCS is obtained.

III. TEST VERIFICATION

A. EXPERIMENT PLATFORM

In order to prove that the SSI risk assessment scheme proposed in this paper can effectively and objectively quantify the SSI risk level of industrial control systems and equipment, we built a typical industrial control safety test platform to verify the effectiveness of the proposed scheme. As shown in Figure 5, the platform is divided into three parts: supervisory control layer, field control layer, and field device layer. The supervisory control layer includes a global operating station, OPC server, main engineer station and clock synchronization server.

In order to test reliability and universality of the scheme in this article, the DCS adopted by the on-site control layer consists of control nodes (including control stations and communication interfaces connected to the process control network with heterogeneous systems, etc), operating nodes (including engineer station, operator station, configuration server (main engineer station), data server and other man-machine conversation interface stations connected to Sonet and Scnet) and system network (including I/O bus, Scnet, Sonet, etc).

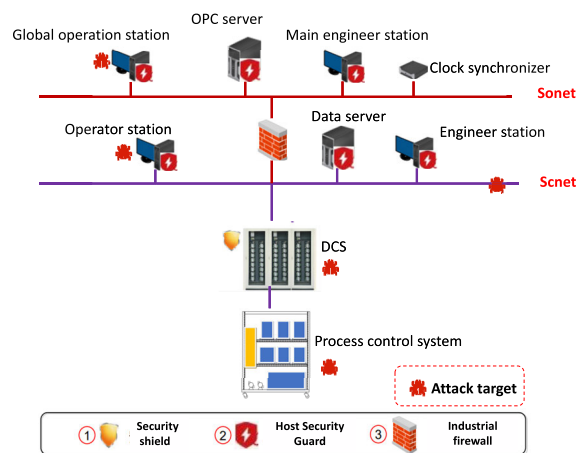


FIGURE 5. (SSI risk assessment scheme) Test platform topology diagram.

Sonet connects all operating nodes such as engineer station, operator station, configuration server (main engineer station) and data server in the control system, and transmits historical data, alarm information and operation records among the operating nodes. For each application site linked to Sonet, real-time and historical information can be accessed through the data server of each operating domain, and operating instructions can be issued. Scnet connects operating nodes and control stations such as engineer stations, operator stations, and data servers, and transmits real-time data and various operating instructions between the operating nodes and control stations.

The software and hardware configuration of the DCS engineer station is shown in Figure 6, including two network cards, the IP address of port A is 128.128.1.130, the IP address of port B is 128.128. 2.130. The engineer station is installed with the AdvanTrol-pro2.7 installation disk of Zhejiang University Suppressor. The installed computer is used as the engineer station to choose the installation engineer station, and as the operator station, choose the installation operator station.

The data flow in the system is that real-time data on the control network is sent to the operating station and the server at the same time. Because the operating station needs to occupy a lot of network bandwidth when querying historical data from the server, the historical data communication of the system is carried out through Sonet, which greatly reduces the network load of Sonet, and the real-time and stability of Scnet can be improved. Similarly, the vulnerability of the system is also reflected in the communication process. Communication failure caused by attacks such as occupying bandwidth will cause the function of entire system to fail.

The experiment takes the communication process between CS4000 water tank system and DCS as the research object. On the basis of conventional PID algorithm to control the liquid level of cascade water tank, the SSI failure mode is applied to the target position of building platform to observe and record the abnormal change of the position number of

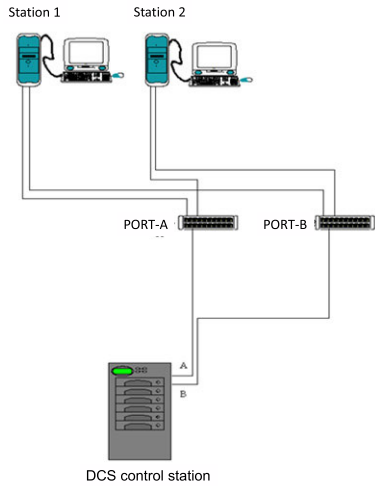


FIGURE 6. (SSI risk assessment scheme) test platform topology diagram.

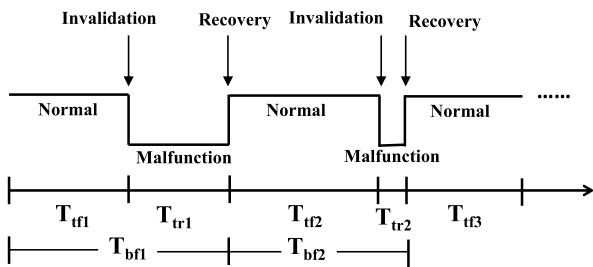


FIGURE 7. RAM time definition.

liquid level working condition that deviates from the normal situation. We rely on host security guards and other security defense methods to complete communication anomaly detection and security failure repair. Among them, multiple sets of offensive and defensive experiments are completed for each failure mode, and process data such as the average time before failure, average time between failures, and average time before recovery are measured through the experiments.

B. VALIDATION VERIFICATION OF ENTROPY WEIGHT OPTIMIZATION SCHEME

Taking the changing trend of tank level of CS4000 system as the observation object, taking into account the robustness of system itself, the attack time interval is set to 5min, and the attack method corresponding to the failure mode is applied to the attack target in Figure 5. Table 7 shows the failure modes of different target positions,

We adjusted the water tank level value from 70% of the maximum level to 40%. The following are the changes in water tank level corresponding to several failure modes. The impact of the communication delay failure mode that is not given is the sum of the effects of other failure modes on control command delay and flow data delay, etc.

We examined the time domain risk index values of the DCS under five failure modes. The size of the broken line in Figure 9(a)(b)(c)(d)(e) reflects the security defense

TABLE 7. Correspondence between target position and failure mode.

| Target Position \ Failure mode | DCS | Engineer station | Process control system | Global operation station | Control network |
|--------------------------------|-----|------------------|------------------------|--------------------------|-----------------|
| Data failure | ✓ | | ✓ | | |
| Data replay | ✓ | | | ✓ | ✓ |
| Data forgery | ✓ | ✓ | | ✓ | ✓ |
| Personnel operation | | ✓ | ✓ | | |
| Communication delay | ✓ | ✓ | ✓ | ✓ | ✓ |

capabilities of the corresponding failure mode. The fluctuation of the broken line means the uncertainty of failure modes, that is, the limitations of the inherent defense and repair methods.

Since multiple failure modes have overlapping effects on multiple safety including liquid level control functions, it is also necessary to investigate the failure detection and precise positioning capabilities of the platform itself, that is, obstacle detection capabilities and obstacle detection accuracy. We add another 200 sets of offensive and defensive experiments for each failure mode, and use the average failure detection rate and false alarm rate to measure this function, and then add the time domain security indicators. The statistics are shown in Table 8

TABLE 8. Risk index data of multiple failure modes of DCS.

| Failure mode \ Risk index | Data failure | Data replay | Data forgery | Personnel operation | Communication delay |
|-----------------------------------|--------------|-------------|--------------|---------------------|---------------------|
| Average time before failure (s) | 251.5 | 242.1 | 237.2 | 239.2 | 251.0 |
| Average time between failures (s) | 298.2 | 300.3 | 300.0 | 298.7 | 300.6 |
| Average time before recovery (s) | 47.7 | 58.2 | 62.9 | 60.7 | 49.6 |
| False alarm rate (%) | 0.036 | 0.008 | 0.312 | 0.176 | 0.452 |
| Mean failure detection rate (%) | 0.928 | 0.9 | 0.704 | 0.908 | 0.992 |

Based on the data in Table 8, we can use the designed entropy weight optimization scheme to calculate the relative importance of various failure modes. Here we still need to analyze the delay effects of the first four failure modes, and quantify the correlation properties between communication delay failure modes.

From equations (2) to (4), the correlation degree $\epsilon_{15} = 0.195$, $\epsilon_{25} = 0.227$, $\epsilon_{35} = 0.274$, $\epsilon_{45} = 0.243$ is obtained respectively, that is, the influence of failure modes is arranged as $3 > 4 > 2 > 1$ on the delay attribute failure. Then, from equations (5) to (13), the importance weights of the first four failure modes and the communication delay failure mode after eliminating the delay effects are obtained, and then

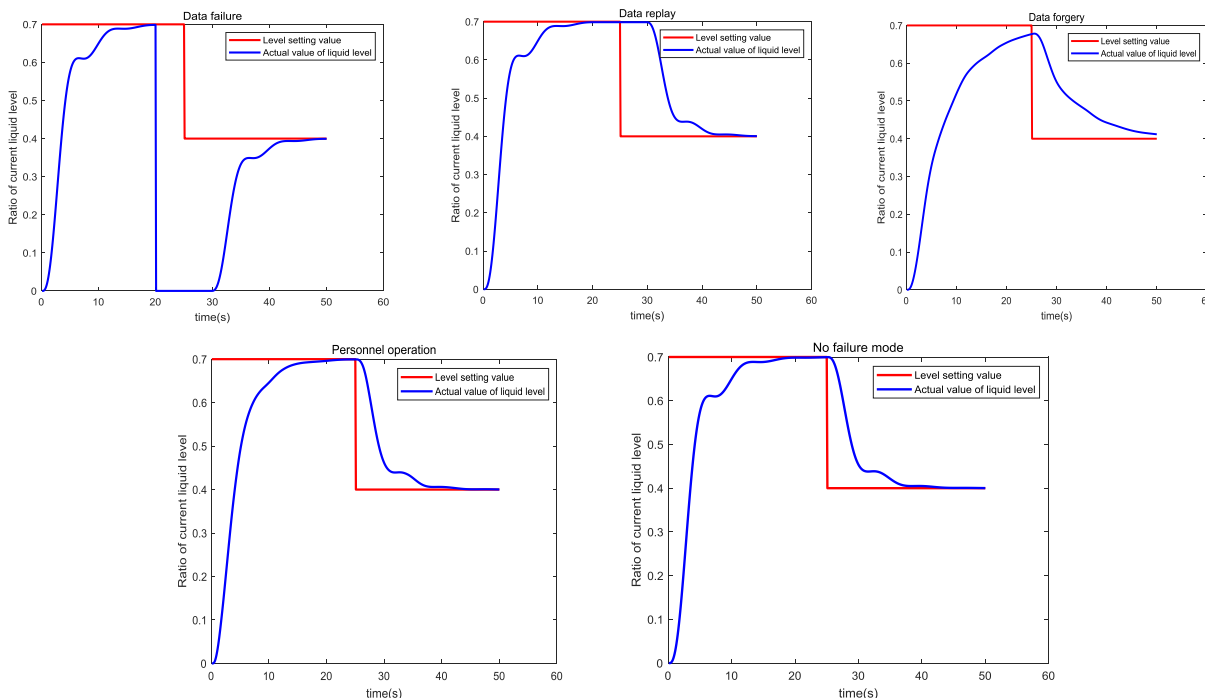


FIGURE 8. The influence of five failure modes on liquid level control function.

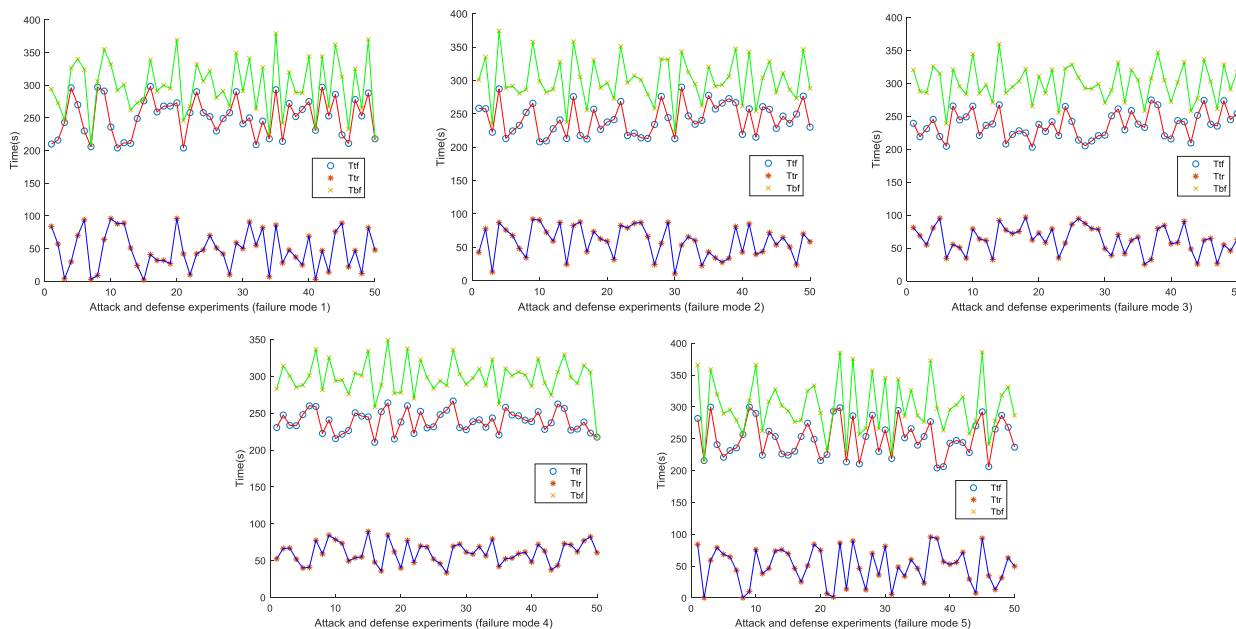


FIGURE 9. Risk index value of the time type under the offensive and defensive process.

the judgment matrix R_{DCS} is obtained from equations (14) to (15):

$$R_{DCS} = \begin{bmatrix} 0.5 & 0.87 & 0.9 & 0.83 & 0.96 \\ 0.13 & 0.5 & 0.62 & 0.4 & 0.85 \\ 0.1 & 0.38 & 0.5 & 0.3 & 0.8 \\ 0.17 & 0.6 & 0.7 & 0.5 & 0.88 \\ 0.04 & 0.15 & 0.2 & 0.12 & 0.5 \end{bmatrix} \quad (22)$$

From equations (16) to (19), the weight vectors of the five failure modes of DCS are obtained:

$$\omega_{DCS} = [0.04, 0.15, 0.2, 0.12, 0.49] \quad (23)$$

We divide the importance dimension into five levels according to the importance difference between failure modes, and obtain the quantitative scale of priority

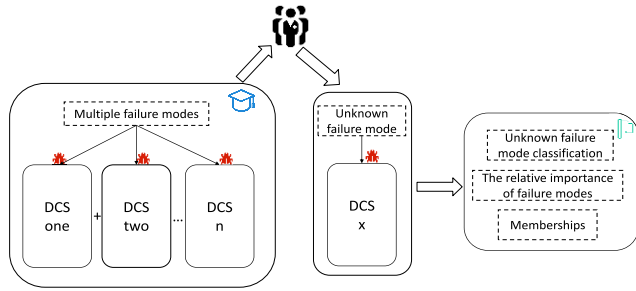


FIGURE 10. Risk index value of the time type under the offensive and defensive process.

relationship judgment matrix accurately and quantified. In order to meet the grade range, take $\eta = 130$ in Table 4, then as shown in Table 9,

TABLE 9. The quantitative scale of the priority relationship judgment matrix of DCS.

| Scaling | Meaning |
|----------------------|--|
| 0.5 | equally important |
| 0.73 | Slightly important (Equal to Mode 4 vs. Mode 1) |
| 0.83 | Obviously important (Equal to Mode 2 vs. Mode 1) |
| 0.9 | Strongly important (Equal to Mode 3 vs. Mode 1) |
| 0.95 | Extremely important (Equal to Mode 5 vs. Mode 1) |
| $\log_{130} i + 0.5$ | The scale when the two adjacent scales are |
| $i = 2, 4, 6, 8$ | compromised |

The risk index data set is divided according to the level, and the membership degree of each failure mode is obtained. In the same way, according to the quantitative priority scale, we approximate the DCS's comment set $E = \{\text{very safe, relatively safe, basic safe, relatively dangerous, very dangerous}\} = \{1, 2, 46, 4.12, 5.92, 7.82\}$, From equation (23), $V'_{DCS} = 2.8735$ is obtained, that is, the program evaluates the DCS safety level to be within the range of relatively safe to basic safe.

C. COMPARATIVE ANALYSIS OF ENTROPY WEIGHT OPTIMIZATION METHOD AND EXPERT EXPERIENCE METHOD

In order to verify the accuracy of the entropy weighting scheme, we also design a safety assessment scheme based on expert experience. We adopt a general priority relationship judgment matrix quantitative scale, that is, define the scale level according to 0.1~0.9 with an interval of 0.1, and invite several representative experts to give the relative importance value and fuzzy membership degree of ECS-700 failure mode according to the evaluation standard based on their own experience.

We use the scattered points to fit the expert's empirical judgment process on the importance of different

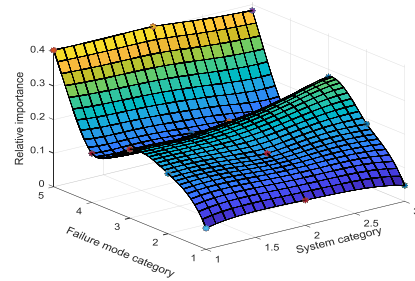


FIGURE 11. The process of determining the importance of failure modes based on expert experience.

failure modes of three DCS systems which are JX300xp, ECS-100 and ECS-700 namely, as shown in Figure 11.

The DCS is composed of system software, hardware, field instruments, etc. Among them, the DCS hardware and software will be frequently upgraded and replaced, and the risk level of the system will also change. Being between adjacent integers in the system category means that it is between the risk level of DCS corresponding to the integer due to the different configuration of DCS, and the same is true for failure modes.

As mentioned above, the failure modes of industrial control systems and equipment are not fixed. When experts classify certain failure modes, their important quantification method is only to weight and combine the known failure modes in the knowledge base according to their experience and way of thinking and then complete the quantification of relative importance. This quantitative method is subjective to a certain extent and lacks a quantitative analysis of the internally related safety-related components of the system. The following is the DCS SSI assessment process based on expert experience, as shown in Table 4, we use the definition of a general scale, that is, select 0.1 to 0.9, with an interval of 0.1 as the importance scale. Judgment matrix under the expert knowledge base:

$$R'_{DCS} = \begin{bmatrix} 0.5 & 0.7 & 0.8 & 0.6 & 0.9 \\ 0.3 & 0.5 & 0.6 & 0.4 & 0.8 \\ 0.2 & 0.4 & 0.5 & 0.4 & 0.8 \\ 0.4 & 0.6 & 0.6 & 0.5 & 0.9 \\ 0.1 & 0.2 & 0.2 & 0.1 & 0.5 \end{bmatrix} \quad (24)$$

The fuzzy membership degree E is:

$$\begin{aligned} E_1 &= \{0, 0.25, 0.35, 0.35, 0.05\} \\ E_2 &= \{0, 0.15, 0.45, 0.3, 0.1\} \\ E_3 &= \{0, 0.12, 0.4, 0.36, 0.12\} \\ E_4 &= \{0, 0.2, 0.38, 0.34, 0.08\} \\ E_5 &= \{0, 0.15, 0.45, 0.22, 0.18\} \end{aligned} \quad (25)$$

Given the unquantified and general fuzzy comment set $E = \{\text{very safe, relatively safe, basic safe, relatively dangerous, very dangerous}\} = \{1, 2, 3, 4, 5\}$, from equation (21), we get $V'_{DCS} = 2.8735$, that is, the expert plan evaluates the ECS-700 system risk level to be within the range of

relatively safety to basic safety, which is basically consistent with the evaluation result of entropy weight optimization plan.

We compare the process of two solutions. The process of the expert experience method is similar to the process of machine learning. By learning a large number of experience samples, each expert will train a knowledge base “model,” and then give the evaluation system safe value. The entropy weight optimization evaluation scheme is to evaluate the risk level of the system through the value of risk indexes on the basis of excluding the association of risk indexes. In contrast, expert experience is an artificial learning process oriented to historical results, and due to subjectivity, the risk factors of certain systems are often overlooked. Entropy weight optimization evaluation can objectively and accurately evaluate the risk level reflected by inherent indicators. However, due to the diversity of failure modes of industrial control systems and equipment, common indicators cannot reflect all their safety characteristics, that is, it is impossible to provide a set of fixed and complete risk indicators to evaluate the SSI risks of the entire system and equipment. It is necessary to combine expert experience to improve the process of increasing and decreasing indicators and updating failure modes in the risk assessment process, so as to obtain the SSI risk assessment value of system and equipment more accurately.

IV. CONCLUSION

In response to the risk assessment requirements of the industrial control system of the integrated architecture of security and safety, this paper designs an SSI industrial control system architecture in which security measures are integrated into safety failure modes, and on this basis, builds a FAHP multi-objective dynamic risk assessment model based on the SSI architecture, and an entropy weight optimization method using the GRA degree to correct the correlation of the index is proposed as a parameter scheme for determining the relative importance of the element layer and the evaluation layer. The experimental results show that the scheme designed in this paper is basically consistent with the SSI assessment results of the system equipment by the expert experience method, but the scheme can reflect the risk level of the system equipment more objectively and quantitatively.

For the method proposed in this article, the work will focus on the following aspects.

1) The SSI is not limited to the communication process level of industrial control system and the modeling of industrial control system needs to be further refined according to actual situation, including more comprehensive SSI sub-models, and more comprehensive attack division for industrial control system and so on.

2) In the comprehensive fuzzy evaluation of the relative importance of each element and the comprehensive fuzzy evaluation of each element of the evaluation layer, the comprehensiveness and accuracy of the risk-related indicators considered need to be defined. How to design a method of

correlation analysis with the expert experience method will also be the focus of research.

REFERENCES

- [1] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, “A survey of approaches combining safety and security for industrial control systems,” *Rel. Eng. Syst. Saf.*, vol. 139, pp. 156–178, Jul. 2015.
- [2] L. González, M. Vaca, and R. Lattarulo, “Análisis de riesgos de ciberseguridad en arquitectura de vehículos automatizados,” in *Proc. XXXIX Jornadas de Automática*, Badajoz, Spain, 2020, pp. 838–845.
- [3] S. Chockalingam, D. Hadžiosmanović, and W. Pieters, “Integrated safety and security risk assessment methods: A survey of key characteristics and applications,” in *Proc. 11th Int. Conf. Crit. Inf. Infrastruct. Secur.*, Paris, France, 2016, pp. 50–62.
- [4] R. Kumar and M. Stoelinga, “Quantitative security and safety analysis with attack-fault trees,” in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng.*, Singapore, Jan. 2017, pp. 25–32.
- [5] K. T. Kosmowski, M. Śliwiński, and E. Piesik, “Integrated safety and security analysis of hazardous plants and systems of critical infrastructure,” *J. Polish Saf. Rel. Assoc.*, vol. 6, no. 2, pp. 31–45, 2015.
- [6] X. Lyu, Y. Ding, and S. Yang, “Safety and security risk assessment in cyber-physical systems,” *IET Cyber, Phys. Syst., Theory Appl.*, vol. 4, no. 3, pp. 221–232, Sep. 2019.
- [7] A. Ellis, “Integrating industrial control system (ICS) safety and security—A potential approach,” in *Proc. 10th IET Syst. Saf. Cyber-Secur. Conf.*, Bristol, U.K., 2015, pp. 1–7.
- [8] K. A. Pettersen and T. Bjørnskau, “Organizational contradictions between safety and security—Perceived challenges and ways of integrating critical infrastructure protection in civil aviation,” *Saf. Sci.*, vol. 71, pp. 167–177, Jan. 2015.
- [9] W. Xiong and J. Jin, “Summary of integrated application of functional safety and information security in industry,” in *Proc. 12th Int. Conf. Rel. Maintainability, Saf.*, Shanghai, China, Oct. 2018, pp. 463–469.
- [10] C. Witkowski, “A pragmatic approach towards safe and secure medical device integration,” in *Proc. Int. Conf. Comput. Saf., Rel., Secur.*, Florence, Italy, 2014, pp. 310–325.
- [11] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, “Security application of failure mode and effect analysis (FMEA),” in *Proc. Int. Conf. Comput. Saf., Rel., Secur.*, Florence, Italy, 2014, pp. 310–325.
- [12] A. Hristova, R. Schlegel, and S. Obermeier, “Security assessment methodology for industrial control system products,” in *Proc. 4th Annu. IEEE Int. Conf. Cyber Technol. Autom., Control Intell.*, Hong Kong, Jun. 2014, pp. 264–269.
- [13] K. Coffey, R. Smith, L. Maglaras, and H. Janicke, “Vulnerability analysis of network scanning on SCADA systems,” *Secur. Commun. Netw.*, vol. 2018, no. 1, pp. 1–20, 2018.
- [14] W. Xin, T. Zuo-Qi, and X. U. Shuo, “Information security risk assessment based on fuzzy theory and BRBPNN,” *Comput. Simul.*, vol. 36, no. 11, pp. 184–189, 2019.
- [15] W. Shang, T. Gong, C. Chen, J. Hou, and P. Zeng, “Information security risk assessment method for ship control system based on fuzzy sets and attack trees,” *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Mar. 2019.
- [16] K. Meng Tay and C. Peng Lim, “Fuzzy FMEA with a guided rules reduction system for prioritization of failures,” *Int. J. Qual. Rel. Manage.*, vol. 23, no. 8, pp. 1047–1066, Oct. 2006.
- [17] W. Song, X. Ming, Z. Wu, and B. Zhu, “A rough TOPSIS approach for failure mode and effects analysis in uncertain environments,” *Qual. Rel. Eng. Int.*, vol. 30, no. 4, pp. 473–486, Jun. 2014.
- [18] M. Rafie and F. S. Namin, “Prediction of subsidence risk by FMEA using artificial neural network and fuzzy inference system,” *Int. J. Mining Sci. Technol.*, vol. 25, no. 4, pp. 655–663, Jul. 2015.
- [19] Y. B. Leau, S. Manickam, and Y. W. Chong, “Network security situation assessment: A review and discussion,” in *Information Science and Applications (Lecture Notes in Electrical Engineering)*, vol. 339, no. 1. Singapore: Springer, 2015, pp. 407–414.
- [20] A. Hassan, M. R. A. Purnomo, and A. R. Anugerah, “Fuzzy-analytical-hierarchy process in failure mode and effect analysis (FMEA) to identify process failure in the warehouse of a cement industry,” *J. Eng., Des. Technol.*, vol. 18, no. 2, pp. 378–388, Sep. 2019.
- [21] H. Yetis and M. Karakose, “Nonstationary fuzzy systems for modelling and control in cyber physical systems under uncertainty,” *Int. J. Intell. Syst. Appl. Eng.*, vol. 7, no. 1, pp. 26–30, 2017.



JUNPENG MI was born in Wuhu, China. He received the B.E. degree in automation from Xi'an Jiaotong University, in 2017. He is currently pursuing the Ph.D. degree with the School of Control Science and Engineering, Zhejiang University.

His research direction is industrial control network security. His research interests include heterogeneous network integration of industrial control systems, intrusion detection, and security and privacy in industrial control network systems.



MENGCHI CHEN received the B.S. degree in communication engineering from Soochow University, Suzhou, China, in 2016. He is currently pursuing the Ph.D. degree in electronics and information with the Institute of Cyber-Systems and Control, Zhejiang University.

His research interests include machine vision, artificial intelligence, and industrial automation transformation technology.



WENJUN HUANG received the B.S. and M.S. degrees in automatics from Zhejiang University, in 1972 and 1975, respectively.

He is currently a Professor with the College of Control Science and Engineering, Zhejiang University. His current research directions include industrial Internet, the Internet of Things, embedded systems, application system-based on artificial intelligence, real-time control, and information management system strategy in distributed environment. He is also a Chartered Engineer of British Engineering Council and a member of the National Professional Standardization Technical Committee.



WEI ZHANG received the B.S. degree in automation from the Zhejiang University of Technology, in 2004, and the master's degree in control engineering from Zhejiang University, in 2012.

He is currently working with the Department of Industrial Communication Technology, Zhejiang Supcon Technology Company Ltd. His research interests include industrial control systems and development and industrial control network security technology.

• • •