IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 24, No. 2, April, 2019, pp. 147-154
Journal homepage: http://iieta.org/journals/isi

# The Reliability Assessment of ICS Based on Evidential Reasoning and Semi-quantitative Information

Yuhe Wang[1], Peili Qiao[1*], Haibin Chen[2], Zhiyong Luo[1], Guanglu Sun[1]

[1] School of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China
[2] Heilongjiang Tobacco Industry Co., Ltd., Harbin 150000, China

Corresponding Author Email: Qiaopl@hrbust.edu.cn

https://doi.org/10.18280/isi.240203

**Received:** 15 December 2018
**Accepted:** 25 January 2019

***Keywords:***
*ER method, industrial control system, reliability assessment, semi-quantitative information*

**ABSTRACT**

The purpose of this paper is to establish a new reliability assessment architecture for Industrial Control system (ICS), in this assessment architecture, precise data, ignorance and fuzziness are all modelled to describe complicated ICS. A method based on evidential reasoning (ER) rule and semi-quantitative information is proposed, this approach can solve the multiple attribute decision analysis problems which are characterized by both quantitative data and qualitative knowledge. The assessment results of a practical case study of ICS which ER employed to transform multiple attributes and verify more accurate assessment results can be obtained. The impacts of the obtained results the security states of the ICS, which enable engineer betters understand the operation of the ICS, and ultimately reduce the failure of the system, and improve the security and stability of the system.

## 1. INTRODUCTION

Industrial control systems (ICS) are commonly used in industries such as electric, oil, pulp, chemical and pharmaceutical as well as other manufacturing, which are integrated with the use of computer technology, communication, and control theory [1]. ICS include supervisory control and data acquisition (SCADA) system, distributed control systems (DCS) and programmable logic controllers (PLC). Manufacturers often focus on the fault of equipment and ignore the availability of ICS. Increasingly, these systems have been connected to corporate networks and thus, the Internet. As a consequence, more cyber-attacks may occur and have drawn persons' attention [2-3]. Nevertheless, the security events of the ICS mainly due to the breakdowns of the internal degradation, and the failure frequency of ICS components may increase over time because of the harsher environment.

When the ICS troubles appear, users probably lose their monitoring and control that may cause the damage of facilities and economic losses. Most seriously, it could lead to casualties. Such key critical infrastructures, of which ICS form the core, need to be available at all times. Continuous availability requires strong measurable assessment to confirm the current state of the system. The essence of reliability evaluation is to obtain reasonable security through the rational integration of multiple attributes [4-6].

However, in an ICS, the failure information of the monitoring equipment is fuzzy and uncertainty [7]. Thus, the corresponding method must handle uncertain information. The method to construct the assessment model of ICS can be divided into three types [8-10]: qualitative knowledge-based model, quantitative information-based model and semi-quantitative information based model. The qualitative knowledge-based model mainly relies on experts knowledge or subjective analysis for assessment, for example [11-14]. Qualitative knowledge is used in these methods to predict, which operates simply and easily. But ICS which is regarded as a complex ICS contains too much uncertain information. It is difficult to build a precise model by using single qualitative knowledge. Relatively, information-based quantitative models like artificial neural network model (ANN) [15], grey theory-based model [16-18] are widely used. These methods use quantitative data to train the parameters of the model that we have built. However, the perdition results may not be accurate when there is a lack of prior knowledge and training samples. Hence, semi-quantitative employed by quantitative and qualitative knowledge is introduced for training which has the advantages in predicting the ICS. For example, Subramanian [19] applied Bayesian Belief Network (BBN) to model components and essential condition of security and safety. A two-stage parallel Hidden Markov Model (HMM) [20] is proposed to predict the transient stability assessment (TSA) of power system. These two methods can solve the probabilistic uncertainty, but they cannot solve the fuzzy uncertainty. Fuzzy Neural Network (FNN) [21] can solve fuzzy uncertain information, and is applied to settle the transient stability assessment problem. But this method cannot solve the probabilistic uncertainty information. Thus, it is necessary to set up an appropriate model of ICS assessment that can both resolve the quantitative and qualitative knowledge with probabilistic uncertainty and fuzzy uncertain information.

The Dempster-Shafer (D-S) theory of evidence provides an approaching framework to model quantitative and qualitative knowledge [22]. Compared with Bayesian inference, D-S can deal with uncertainty owing to the limitation of expert abilities or prior knowledge. Then, ER method is proposed as a Multi-Criteria Decision Analysis (MCDA) approach based on belief decision and D-S theory. It has been widely used in many fields such as cloud computing [23], disease predicting [24], Network assessment [25]. The assessment of SCADA has different types of information needed to be integrated which

ER rule has the advantage of solving the conflict of evidence by using focal elements. Above all, the paper uses ER rule to set up a reliability assessment model of the SCADA including three aspects is proposed. And then give a case study based on a real SCADA by using the proposed method.

Herein, the paper introduces the architecture of ICS in Section II. Section III introduces ER method to build a new reliability assessment architecture based on a real productive enterprise in Heilongjiang, China. Section IV illustrates a practical case study for SCADA mentioned above, and analyses simulation results using ER rule. Finally, conclude the paper in Section V.

## 2. THE ARCHITECTURE OF ICS

The ICS consists of hardware, software. Based on several studies such as those described by Igure [26] and Hentea [27] that have focused on ICS architecture, the ICS General Layout as Figure 1.

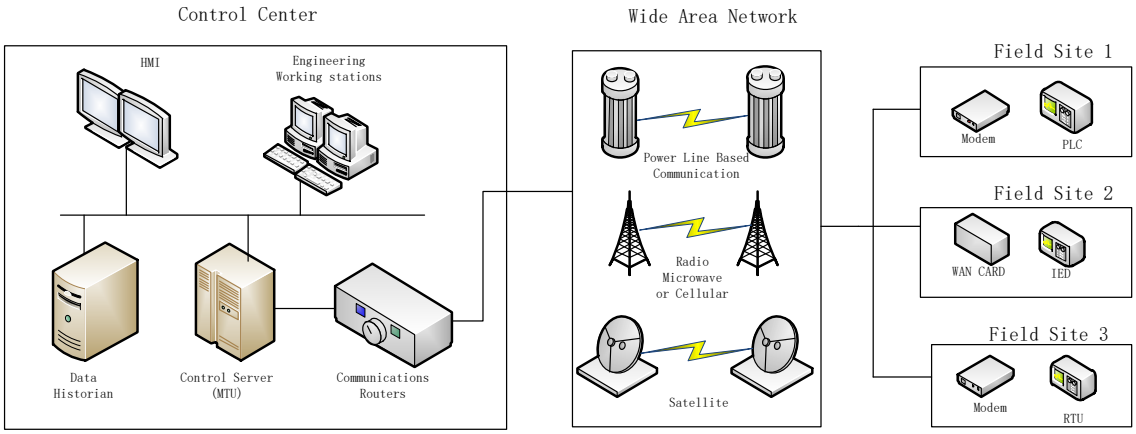


**Figure 1.** ICS general layout

Figure 1 shows the main components and general configuration of an ICS. Typical hardware of ICS includes an MTU placed in control center, RTU or PCL which used to control computer or monitoring sensor. The main function of RTU and PLC is to control the local process, and MTU stores and processes the input and output information of RTU.

The software of the ICS tells when to monitor and control the system. The engineer inputs the system monitoring components as required and determines the range of acceptable parameters and what protection and response to start when the parameters exceed the acceptable values. ICSs are frequently designed to be fault-tolerant, with an army of redundancy built into the system. For example, the ICS server can communicate directly with IEDS or query and collect IED data through local RTU. In most cases, IEDS can work without a control instruction, based on pre-entered parameters. In addition, the control center includes ICS servers, communication routers, HMI, Working Stations, and history databases.

The control center is mainly responsible for collecting alarm information, analysis of trend and report as well as on-site real-time information, which is displayed through HMI and can be generated according to the detected events. Operators can make remote diagnosis and repair through on-site modems or through serial communication (e.g. telephone lines, cables, optical fiber, broadcasting, microwave and satellite, etc.) in the control center.

## 3. RELIABILITY ASSESSMENT OF ICS

In ICS, most production processes require all time monitoring, operation and control. These processes can be loss of control if the hardware of ICS fails. The task of assessing the reliability of the ICS starts with the identification of all faults events that may take place at each of the monitored and controlled components, which require attention and intervention of system operators.

In this section, the evaluation attributes can be divided into two categories: quantitative data and qualitative knowledge. Quantitative data can be represented as a certain amount, quantity, or range of data, such as the duration of the system, the frequency of component failures, and the fault tolerance rate of PLC. These attributes can be collected by the data monitoring system. However, qualitative knowledge is related to the subjective quality of situations or phenomena, such as the consequences of component failures, controllability of access terminals, integrity of controls, and stability of communications. Qualitative knowledge is abstract and it either doesn't need to be measured, or it cannot be measured, because the reality they represent can only be approximated. Therefore, decisions may be related to uncertainty. Because these knowledge is acquired through observation and interpretation to understand the combination of, the uncertainty is often happen, because the information has not been clearly described, or only partially and imprecise evidence to describe, such as personalized service ability and the ability of disaster recovery. ER rule can make full use of qualitative knowledge and quantitative data, and also can express various uncertainties. In this section, a new reliability assessment architecture is established, including three aspects, and then ER rules are used to evaluate the reliability of ICSs.

### 3.1 The basic attributes of ICS reliability

A four-level reliability attributes structure of cloud computing platform is established, including both quantitative data and qualitative knowledge. Reliability of cloud computing platform is categorized in 3 distinct aspects: hardware reliability, software reliability and communication reliability. For each attribute, the symbol "*r*" is numerically labeled according to the hierarchy, while the symbol "*t*" is

valued as the weight which is one of the important parameters in the process of ER rule. In the aspect of the network reliability, all the attributes are measured as the quantitative data, thus most of attributes are defined as a qualitative knowledge. In this paper, we introduce a four-grade assessment levels as the frame of discernment of the reliability assessment model. The ICS reliability is shown in Table 1.

**Table 1.** The basic attributes reliability of SCADA system

| Reliability | 1st level | 2nd level | 3rd level | 4th level |
|---|---|---|---|---|
| The reliability of SCADA system ($R$) | Software Reliability of SCADA system($r_1$)($t_1$=0.2) | Reliability of software($r_{11}$)($t_{11}$=0.2) | Software Error Frequence($r_{111}$)($t_{111}$=0.3) | |
| | | | Software Error Consequence($r_{112}$)($t_{112}$=0.4) | |
| | | | Duration Time of the Software ($r_{113}$)($t_{113}$=0.3) | |
| | | Reliability of Operation System($r_{12}$)($t_{12}$=0.2) | Frequence of Errors in Operation System($r_{121}$)($t_{121}$=0.25) | |
| | | | Consequence of Error in Operation System($r_{122}$)($t_{122}$=0.3) | |
| | | | Bugs in Operation System ($r_{123}$)($t_{123}$=0.15) | |
| | | | Duration of the Operation System($r_{124}$)($t_{124}$=0.3) | |
| | | Reliability of Database($r_{13}$)($t_{13}$=0.25) | Database Error($r_{131}$)($t_{131}$=0.5) | Frequency of Error in Database ($r_{1311}$)($t_{1311}$=0.3) |
| | | | | Consequence of Error in Database ($r_{1312}$)($t_{1312}$=0.4) |
| | | | | Fault tolerant rate of Database ($r_{1313}$)($t_{1313}$=0.3) |
| | | | Data Integrity($r_{132}$)($t_{132}$=0.5) | |
| | | Reliability of Other Hardware($r_{14}$)($t_{14}$=0.35) | Controllability of Access ($r_{141}$)($t_{141}$=0.3) | Frequency of Aceess Error in PLC($r_{1411}$)($t_{1411}$=0.3) |
| | | | | Frequency of Writing Error in PLC($r_{1412}$)($t_{1412}$=0.3) |
| | | | | Frequency of Reading Error in PLC($r_{1413}$)($t_{1411}$=0.4) |
| | | | Stability of PLCs ($r_{142}$)($t_{142}$=0.4) | |
| | Hardware Reliability ($r_2$)($t_2$=0.5) | Hardware Reliability of HMI | Frequency of failure($r_{211}$)($t_{211}$=0.3) | |
| | | | Consequence of Failure($r_{212}$)($t_{212}$=0.4) | |
| | | | Fault tolerant rate of Hardware($r_{213}$)($t_{213}$=0.3) | |
| | | Hardware Reliability of Engineering Working Station | Frequency of failure in PLCs($r_{221}$)($t_{221}$=0.2) | |
| | | | Consequence of Failure PLCs($r_{222}$)($t_{222}$=0.3) | |
| | | | Fault tolerant rate of PLCs($r_{223}$)($t_{223}$=0.3) | Time Between Failures in PLC($r_{2231}$)($t_{2231}$=0.5) |
| | | | | Time to Restore System ($r_{2232}$)($t_{2232}$=0.5) |
| | | | Duration Time of PLCs($r_{224}$)($t_{224}$=0.2) | |
| | Communication Reliability ($r_1$)($t_1$=0.3) | Reliability of ProfiBUS | Frequency of failure in ProfiBUS($r_{311}$) ($t_{311}$=0.4) | |
| | | | Consequence of Failure in ProfiBUS($r_{312}$) ($t_{312}$=0.6) | |
| | | Reliability of Profinet | Frequency of failure in ProfiBUS($r_{321}$) ($t_{321}$=0.4) | |
| | | | Consequence of Failure in ProfiBUS($r_{322}$) ($t_{322}$=0.4) | |

### 3.2 The assessment grades of the attributes

The evaluation grade of ICS attributes was established. For quantitative attributes, the data range is divided into four grades, which is determined as excellent summary establishes the assessment grade of ICS attributes". For quantitative attributes, the data range is divided into four grades, which are determined as "excellent (A), good (B), common (C) and bad (D)". Through the expert experience and the actual investigation, the quantitative attribute setting is obtained, which ensures the accuracy and traceability of the data. In terms of qualitative attributes, the evaluation level can be determined by experts based on experience or investigation. Evaluation rules can be established by evaluation levels, as shown in Table 2.

**Table 2.** The reference values of the assessment grades

| | D | C | B | A |
|---|---|---|---|---|
| $r_{111}$ | 15 times/day | 10 times/day | 5 times/day | 0 times/day |
| $r_{112}$ | Given by Experts | | | |
| $r_{113}$ | 3 hours | 12 hours | 21 hours | 30 hours |
| $r_{121}$ | 45 times/day | 30 times/day | 15 times/day | 0 times/day |
| $r_{122}$ | Given by Experts | | | |
| $r_{123}$ | 3 times/day | 2 times/day | 1 times/day | 0 times/day |
| $r_{124}$ | 20days | 40days | 60days | 80days |
| $r_{1311}$ | 12 times/month | 8 times/month | 4 times/month | 0 times/month |
| $r_{1312}$ | Given by Experts | | | |
| $r_{1313}$ | Given by Experts | | | |
| $r_{132}$ | Given by Experts | | | |
| $r_{1411}$ | 210 times/hour | 140 times/hour | 70 times/hour | 0 times/hour |
| $r_{1412}$ | 90 times/hour | 60 times/hour | 30 times/hour | 0 times/hour |
| $r_{1413}$ | 300 times/hour | 200 times/hour | 100 times/hour | 0 time s/hour |
| $r_{142}$ | Given by Experts | | | |
| $r_{211}$ | 9times/month | 6times/month | 3times/month | 0times/month |
| $r_{212}$ | Given by Experts | | | |
| $r_{213}$ | Given by Experts | | | |
| $r_{221}$ | 12times/kh | 8times/kh | 4times/kh | 0times/kh |
| $r_{222}$ | Given by Experts | | | |
| $r_{2231}$ | 300h | 600h | 900h | 1200h |
| $r_{2232}$ | 30min/times | 60min/times | 90min/times | 120min/times |
| $r_{224}$ | 1kh | 2kh | 3kh | 4kh |
| $r_{311}$ | 6times/kh | 4times/kh | 2times/kh | 0times/kh |
| $r_{312}$ | Given by Experts | | | |
| $r_{321}$ | 9times/kh | 6times/kh | 3times/kh | 0times/kh |
| $r_{322}$ | Given by Experts | | | |

### 3.3 The reliability assessment based on ER rule

As mentioned above, ER rules can integrate different types of information, including qualitative knowledge and quantitative data. It can also express various uncertainties, such as fuzzy uncertainty, probability uncertainty and ignorance. The basic principles of ER rule are introduced in this section.

Assume that $\{r_1, r_2, \ldots, r_m\}$ of a general attribute $R$ in a two-level hierarchy, and $\{t_1, t_2, \ldots, t_m\}$ denotes the weights of the basic attributes, where $0<t_m<1$,There are $N$ assessment grades,

The belief degree should be converted into the basic probability mass. The process is shown as follows. then the basic step of the ER rule can be concluded as follows:

**Step 1.** The belief degree should be converted into the basic probability mass. The process is shown as follows.

$$
\begin{aligned}
&Q_{i,j} = t_i \beta_{i,j} \\
&Q_{i,\Theta} = 1 - t_i \sum_{j=1}^{N} \beta_{i,j} \\
&\overline{Q}_{i,\Theta} = 1 - t_i \\
&Q_{i,\Theta} = t_i \left( 1 - \sum_{j=1}^{N} \beta_{i,j} \right)
\end{aligned}
\tag{1}
$$

Among them, $Q_{i,j}$ says relative to the first $j$ a quality evaluation grades of basic probability, $Q_{i,\Theta}$ said the evaluation of the $I$ set the basic probability of set, the results the $i$th a not assigned the remaining probability of attribute, there is $Q_{i,\Theta} = \overline{Q}_{i,\Theta} + Q_{i,\Theta}$. Denotes the unallocated basic probability mass relative to the insignificance of the $i$th underlying attribute. $Q_{i,\Theta}$ represents the unallocated base probability mass relative to the incompleteness of the $i$th base attribute.

**Step 2.** The probability quality of the $J$th evaluation grade can be obtained by combining the first I basic attributes with the evidence theory. The detailed steps are as follows:

$$
\begin{aligned}
&Q_{I(i+1),j} = K_{I(i+1)} \left[ Q_{I(i),j} Q_{i+1,j} + Q_{I(i),j} Q_{i+1,\Theta} + Q_{I(i),\Theta} Q_{i+1,j} \right] \\
&Q_{I(i),\Theta} = \overline{Q}_{I(i),\Theta} + Q_{I(i),\Theta} \\
&Q_{I(i+1),\Theta} = K_{I(i+1)} \left[ Q_{I(i),\Theta} Q_{i+1,\Theta} + Q_{I(i),\Theta} \overline{Q}_{i+1,\Theta} + \overline{Q}_{I(i),\Theta} Q_{i+1,\Theta} \right] \\
&\overline{Q}_{I(i+1),\Theta} = K_{I(i+1)} \left[ \overline{Q}_{I(i),\Theta} \overline{Q}_{i+1,\Theta} \right]
\end{aligned}
\tag{2}
$$

where $Q_{I(i),j}$ represents the probability quality of the $J$th evaluation grade after the combination of the first $i$ basic attributes. It can be calculated by formula above:

$$
K_{I(i+1)} = \frac{1}{1 - \sum_{k=1}^{N} \sum_{\substack{j=1 \\ j \neq k}}^{N} Q_{I(i),k} Q_{i+1,j}} \tag{3}
$$

**Step 3.** Finally, based on the obtained probability quality, the confidence of the *J*th evaluation grade and the remaining confidence of the unset evaluation result are calculated as follows:

$$\beta_j = \frac{Q_{I(M),j}}{1-\overline{Q}_{I(M),\Theta}} \quad (j=1,2,\cdots,N)$$
$$\beta_\Theta = \frac{Q_{I(M),\Theta}}{1-\overline{Q}_{I(M),\Theta}} \tag{4}$$

### 3.4 The belief degree of the attributes

When all the values of indicator attributes are determined, the corresponding confidence of the evaluation results should be calculated next. The formula is as follows:

$$\begin{aligned}
&\beta_{i,j} = \frac{R_{i,j+1}-U(r_i)}{R_{i,j+1}-R_{i,j}}(R_{i,j+1} \le U(r_i) \le R_{i,j}) \\
&\beta_{i,j+1} = 1-\beta_{i,j} \\
&\beta_{i,j} = 0(k=1,\cdots,N,k\ne j,j+1)
\end{aligned} \tag{5}$$

where $U(r_i)$ represents the value of the attribute $r_i$, $R_{i,j}$ represents the reference $j$ value of the attribute $r_i$ at the first evaluation level.

By using the monitor to extract the original data of the security index from the cloud system, the attributes of each index are fused step by step.

First, mix 4 indicators, through fusion after 4 index results follow the dimensions in the classification of third-level indexes of three-level index, and according to the third level indicators of merged results fusion in order to get the second cloud security reliability status indicators evaluation level.

Secondly, according to the evaluation result of the second level index after the fusion, the cloud security evaluation grade of the third dimension of the first level is obtained.

Finally, the index data of these three dimensions are finally fused by using ER algorithm again to obtain the reliability and security evaluation level of the overall ICS.

According to the confidence of each evaluation level, we can get the macroscopic reliability and security state of cloud computing system under the current state.

## 4. CASE STUDY

In order to illustrate the detailed process of the reliability assessment, a case which uses the proposed reliability assessment architecture and ER rule to assess the reliability of an actual ICS is studied in this section.

### 4.1 The actual ICS

In this case, a ICS of cigarette factory in Heilongjiang is investigated. The architecture of the platform can be divided into 3 types conclude:

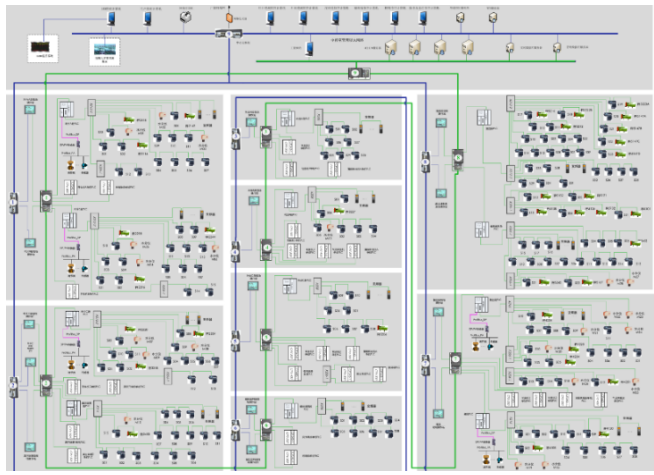

**Figure 2.** Architecture of supervisory control and data acquisition system

### 4.2 The process of the reliability assessment

$$\begin{aligned}
&\beta_{1211,1}=0.8,\ \beta_{1211,2}=0.2,\ \beta_{1211,3}=0,\ \beta_{1211,4}=0 \\
&\beta_{1212,1}=0.7,\ \beta_{1212,2}=0.3,\ \beta_{1212,3}=0,\ \beta_{1212,4}=0 \\
&\beta_{1213,1}=0.2,\ \beta_{1213,2}=0.8,\ \beta_{1213,3}=0,\ \beta_{1213,4}=0 \\
&\beta_{1214,1}=0.9,\ \beta_{1214,2}=0.1,\ \beta_{1214,3}=0,\ \beta_{1214,4}=0
\end{aligned} \tag{6}$$

Then, according to the weight given by formula and Table 1, convert the above confidence degree into the basic probability quality, as follows:

$$\begin{aligned}
&P_{1211,1}=0.32,\ P_{1211,2}=0.08,\ P_{1211,3}=0,\ P_{1211,4}=0,\ P_{1211,\Theta}=0.6,\ \overline{P}_{1211,\Theta}=0.6,\ P_{1211,\Theta}=0 \\
&P_{1212,1}=0.21,\ P_{1212,2}=0.09,\ P_{1212,3}=0,\ P_{1212,4}=0,\ P_{1212,\Theta}=0.7,\ \overline{P}_{1212,\Theta}=0.7,\ P_{1212,\Theta}=0 \\
&P_{1213,1}=0.04,\ P_{1213,2}=0.16,\ P_{1213,3}=0,\ P_{1213,4}=0,\ P_{1213,\Theta}=0.8,\ \overline{P}_{1213,\Theta}=0.8,\ P_{1213,\Theta}=0 \\
&P_{1214,1}=0.09,\ P_{1214,2}=0.01,\ P_{1214,3}=0,\ P_{1214,4}=0,\ P_{1214,\Theta}=0.9,\ \overline{P}_{1214,\Theta}=0.9,\ P_{1214,\Theta}=0
\end{aligned} \tag{7}$$

Then, according to the above attributes, in order to fuse the probability quality, the scale factor should be calculated: $K_{I(i+1)}=K_{I(1212)}$:

$$K_{I(1212)} = \frac{1}{1-\sum_{k=1}^{N}\sum_{\substack{j=1\\ j\ne k}}^{N} P_{I(1211),k}P_{1212,j}} = \frac{1}{1-0.32\times0.09+0.08\times0.21} = 1.0478 \tag{8}$$

Then, the probabilistic quality of the fusion is calculated according to formulas:

$$
\begin{aligned}
P_{I(1212),1} &= K_{I(1212)}\left[P_{I(1211),1}P_{1212,1} + P_{I(1211),1}P_{1212,\Theta} + P_{I(1211),\Theta}P_{1212,1}\right] \\
&= 1.0478\times\left[0.32\times 0.21 + 0.32\times 0.7 + 0.6\times 0.21\right] \\
&= 0.4371 \\
P_{I(1212),2} &= K_{I(1212)}\left[P_{I(1211),2}P_{1212,2} + P_{I(1211),2}P_{1212,\Theta} + P_{I(1211),\Theta}P_{1212,2}\right] \\
&= 1.0478\times\left[0.08\times 0.09 + 0.08\times 0.7 + 0.6\times 0.09\right] \\
&= 0.1228 \\
P_{I(1212),3} &= K_{I(1212)}\left[P_{I(1211),3}P_{1212,3} + P_{I(1211),3}P_{1212,\Theta} + P_{I(1211),\Theta}P_{1212,3}\right] \\
&= 1.0478\times\left[0\times 0 + 0\times 0.7 + 0.6\times 0\right] \\
&= 0 \\
P_{I(1212),4} &= K_{I(1212)}\left[P_{I(1211),4}P_{1212,4} + P_{I(1211),4}P_{1212,\Theta} + P_{I(1211),\Theta}P_{1212,4}\right] \\
&= 1.0478\times\left[0\times 0 + 0\times 0.7 + 0.6\times 0\right] \\
&= 0 \\
P_{I(1212),\Theta} &= K_{I(1212)}\left[P_{I(1211),\Theta}P_{1212,\Theta} + P_{I(1211),\Theta}\overline{P}_{1212,\Theta} + \overline{P}_{I(1211),\Theta}P_{1212,\Theta}\right] \\
&= 1.0478\times\left[0\times 0 + 0\times 0.7 + 0.6\times 0\right] \\
&= 0 \\
\overline{P}_{I(1212),\Theta} &= K_{I(1212)}\left[\overline{P}_{I(1211),\Theta}\overline{P}_{1212,\Theta}\right] \\
&= 1.0478\times\left[0.6\times 0.7\right] \\
&= 0.4401 \\
P_{I(1212),\Theta} &= \overline{P}_{I(1212),\Theta} + P_{I(1212),\Theta} = 0.4401
\end{aligned}
\tag{9}
$$

Then, the scale factor of the third-level index is calculated as follows:

$$
K_{I(1213)} = \frac{1}{1-\sum_{k=1}^{N}\sum_{\substack{j=1\\ j\neq k}}^{N} P_{I(1212),k}P_{1213,j}} = \frac{1}{1-0.4371\times 0.16+0.1228\times 0.04} = 1.0809 \tag{10}
$$

Therefore, the probability quality of the third-level indicator fusion is obtained as follows:

$$
\begin{aligned}
P_{I(1213),1} &= K_{I(1213)}\left[P_{I(1212),1}P_{1213,1} + P_{I(1212),1}P_{1213,\Theta} + P_{I(1212),\Theta}P_{1213,1}\right] \\
&= 1.0809\times\left[0.4371\times 0.04 + 0.4371\times 0.8 + 0.4401\times 0.04\right] \\
&= 0.4159 \\
P_{I(1213),2} &= K_{I(1213)}\left[P_{I(1212),2}P_{1213,2} + P_{I(1212),2}P_{1213,\Theta} + P_{I(1212),\Theta}P_{1213,2}\right] \\
&= 1.0809\times\left[0.1228\times 0.16 + 0.1228\times 0.8 + 0.4401\times 0.16\right] \\
&= 0.2035 \\
P_{I(1213),3} &= K_{I(1213)}\left[P_{I(1212),3}P_{1213,3} + P_{I(1212),3}P_{1213,\Theta} + P_{I(1212),\Theta}P_{1213,3}\right] \\
&= 1.0809\times\left[0\times 0 + 0\times 0.8 + 0.4401\times 0\right] \\
&= 0 \\
P_{I(1213),4} &= K_{I(1213)}\left[P_{I(1212),4}P_{1213,4} + P_{I(1212),4}P_{1213,\Theta} + P_{I(1212),\Theta}P_{1213,4}\right] \\
&= 1.0809\times\left[0\times 0 + 0\times 0.8 + 0.4401\times 0\right] \\
&= 0 \\
P_{I(1213),\Theta} &= K_{I(1213)}\left[P_{I(1212),\Theta}P_{1213,\Theta} + P_{I(1212),\Theta}\overline{P}_{1213,\Theta} + \overline{P}_{I(1212),\Theta}P_{1213,\Theta}\right] \\
&= 1.0809\times\left[0\times 0 + 0\times 0.8 + 0.4401\times 0\right] \\
&= 0 \\
\overline{P}_{I(1213),\Theta} &= K_{I(1213)}\left[\overline{P}_{I(1212),\Theta}\overline{P}_{1213,\Theta}\right] \\
&= 1.0809\times\left[0.4401\times 0.8\right] \\
&= 0.3806 \\
P_{I(1213),\Theta} &= \overline{P}_{I(1213),\Theta} + P_{I(1213),\Theta} = 0.3806
\end{aligned}
\tag{11}
$$

Then, calculate the scale factor of the fourth level indicator, as follows:

$$
K_{I(1214)} = \frac{1}{1-\sum_{k=1}^{N}\sum_{\substack{j=1\\ j\neq k}}^{N} P_{I(1213),k}P_{1214,j}} = \frac{1}{1-0.4159\times 0.01+0.2035\times 0.09} = 1.0230 \tag{12}
$$

Therefore, the probability quality of the fusion of the fourth level indicator is as follows:

$$
\begin{aligned}
P_{I(1214),1} &= K_{I(1214)}\left[P_{I(1213),1}P_{1214,1} + P_{I(1213),1}P_{1214,\Theta} + P_{I(1213),\Theta}P_{1214,1}\right] \\
&= 1.0230\times\left[0.4159\times 0.09 + 0.4159\times 0.9 + 0.3806\times 0.09\right] \\
&= 0.4563 \\
P_{I(1214),2} &= K_{I(1214)}\left[P_{I(1213),2}P_{1214,2} + P_{I(1213),2}P_{1214,\Theta} + P_{I(1213),\Theta}P_{1214,2}\right] \\
&= 1.0230\times\left[0.2035\times 0.01 + 0.2035\times 0.9 + 0.3806\times 0.01\right] \\
&= 0.1933 \\
P_{I(1214),3} &= K_{I(1214)}\left[P_{I(1213),3}P_{1214,3} + P_{I(1213),3}P_{1214,\Theta} + P_{I(1213),\Theta}P_{1214,3}\right] \\
&= 1.0230\times\left[0\times 0 + 0\times 0.9 + 0.3806\times 0\right] \\
&= 0 \\
P_{I(1214),4} &= K_{I(1214)}\left[P_{I(1213),4}P_{1214,4} + P_{I(1213),4}P_{1214,\Theta} + P_{I(1213),\Theta}P_{1214,4}\right] \\
&= 1.0230\times\left[0\times 0 + 0\times 0.9 + 0.3806\times 0\right] \\
&= 0 \\
P_{I(1214),\Theta} &= K_{I(1214)}\left[P_{I(1213),\Theta}P_{1214,\Theta} + P_{I(1213),\Theta}\overline{P}_{1214,\Theta} + \overline{P}_{I(1213),\Theta}P_{1214,\Theta}\right] \\
&= 1.0230\times\left[0\times 0 + 0\times 0.9 + 0.3806\times 0\right] \\
&= 0 \\
\overline{P}_{I(1214),\Theta} &= K_{I(1214)}\left[\overline{P}_{I(1213),\Theta}\overline{P}_{1214,\Theta}\right] \\
&= 1.0230\times\left[0.3806\times 0.9\right] \\
&= 0.3504 \\
P_{I(1214),\Theta} &= \overline{P}_{I(1214),\Theta} + P_{I(1214),\Theta} = 0.3504
\end{aligned}
\tag{13}
$$

Finally, the confidence that the result is obtained after the fusion of the four levels of indicators can be calculated by equations:

$$
\begin{aligned}
\beta_1 &= \frac{P_{I(1214),1}}{1-\overline{P}_{I(1214),\Theta}} = \frac{0.4563}{1-0.3504} = \frac{0.4563}{0.6496} = 0.7024 \\
\beta_2 &= \frac{P_{I(1214),2}}{1-\overline{P}_{I(1214),\Theta}} = \frac{0.1933}{1-0.3504} = \frac{0.1933}{0.6496} = 0.2976 \\
\beta_3 &= \frac{P_{I(1214),3}}{1-\overline{P}_{I(1214),\Theta}} = \frac{0}{1-0.3504} = 0 \\
\beta_4 &= \frac{P_{I(1214),4}}{1-\overline{P}_{I(1214),\Theta}} = \frac{0}{1-0.3504} = 0 \\
\beta_\Theta &= \frac{P_{I(1214),\Theta}}{1-\overline{P}_{I(1214),\Theta}} = \frac{0}{1-0.3504} = 0
\end{aligned}
\tag{14}
$$

## 5. CONCLUSION

Considering the complex properties of ICS, the reliability of ICS is evaluated by using ER rule. ER rules perform well in multiple attribute decisions. It can deal with evidence of high conflict and complete conflict and then make more accurate assessments. On this basis, a reliability evaluation structure of ICS based on multi-attribute decision making is proposed. The reliability attribute of level 4 mainly includes three aspects of software and hardware, which can fully express the reliability of ICS. In conclusion, the innovation points of this paper can be summarized as follows: firstly, the reliability evaluation model of ICS is established by using ER rule. A new reliability evaluation system structure is proposed, including three aspects. Therefore, the above two innovative studies have a good effect on reliability evaluation of complex circuits.

## ACKNOWLEDGMENT

This work was supported in part by the Scientific Research Starting Foundation for Returned Overseas of Heilongjiang Province under Grants LC2018030.

## REFERENCES

[1] Stouffer, K.A., Falco, J.A., Scarfone, K.A. (2008). Guide to industrial control systems (ICS) security: Supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC). Guide to Industrial Control Systems Security.

[2] Huang, K., Zhou, C., Tian, Y.C., Yang, S.H., Qin, Y.Q. (2018). Assessing the physical impact of cyber-attacks on industrial cyber-physical systems. IEEE Transactions on Industrial Electronics, 65(10): 8153-8162. https://doi.org/10.1109/TIE.2018.2798605

[3] Housh, M., Ohar, Z. (2018). Model-based approach for cyber-physical attack detection in water distribution systems. Water Research, 139: 132-143. https://doi.org/10.1016/j.watres.2018.03.039

[4] Eskandarpour, R., Khodaei, A. (2016). Machine learning based power grid outage prediction in response to extreme events. IEEE Transactions on Power Systems, 32(4): 3315-3316. https://doi.org/10.1109/TPWRS.2016.2631895

[5] Luo, Z.Y., You, B., Liu, J.H., Su, J. (2016). Research of the intrusion tolerance state transition system based on semi-markov. Transactions of Beijing Institute of Technology, 36(7): 712-717. http://dx.doi.org/10.15918/j.tbit1001-0645.2016.07.010

[6] Wang, J., Wang, J., Roberts, C., Chen, L. (2015). Parallel monitoring for the next generation of train control systems. IEEE Transactions on Intelligent Transportation Systems, 16(1): 330-338. https://doi.org/10.1109/TITS.2014.2332160

[7] Piluso, C., Huang, J., Liu, Z., Huang, Y. (2010). Sustainability assessment of industrial systems under uncertainty: A fuzzy logic based approach to short-term to midterm predictions. Industrial & Engineering Chemistry Research, 49(18): 8633-8643. http://dx.doi.org/10.1021/ie100164r

[8] Luo, Z.Y., You, B., Xu, J.Z., Liang, Y. (2014). Automatic recognition model of intrusive intention based on three layers attack graph. Journal of Jilin University, 44(5): 1392-1397. http://dx.doi.org/10.7964/jdxbgxb201405027

[9] Chen, Q., Abercrombie, R.K., Sheldon, F.T. (2015). Risk assessment for industrial control systems quantifying availability using mean failure cost (MFC). Journal of Artificial Intelligence & Soft Computing Research, 5(3): 205-220.

[10] Mahalik, N.P., Au, T. (2010). LCDA from industrial systems using control network: A monitoring and assessment scheme for sustainability. Environmental Progress & Sustainable Energy, 27(1): 66-78. http://dx.doi.org/10.1002/ep.10247

[11] Johnson, C. (2011). Using assurance cases and Boolean logic driven Markova processes to formalise cyber security concerns for safety-critical interaction with global navigation satellite systems. Proceedings of Formal Methods for Interactive Systems Workshop, 45: 1-18. http://dx.doi.org/10.14279/tuj.eceasst.45.679.697

[12] Das, L., Rengaswamy, R., Srinivasan, B. (2017). Data mining and control loop performance assessment: The multivariate case. Aiche Journal, 63(8): 3311-3328. http://dx.doi.org/10.1002/aic.15689

[13] Cao, X., Wei, C., Li, J., Yang, L., Zhang, D., Tang, G. (2012). The geological disasters defense expert system of the massive pipeline network SCADA system based on FNN. Asia-Pacific Web Conference, pp. 19-26. http://dx.doi.org/10.1007/978-3-642-29426-6_4

[14] Tang, F., Wang, B., Zha, X., Ma, Z., Shao, Y. (2013). Power system transient stability assessment based on two-stage parallel hidden markov model. Proceedings of the Csee, 33(10): 90-97.

[15] Fang, T., Zhang, R., Gao, F. (2017). LQG benchmark based performance assessment of IMC-PID temperature control system. Industrial & Engineering Chemistry Research, 56(51): 15102-15111. http://dx.doi.org/10.1021/acs.iecr.7b03991

[16] Morland, V. (2002). Monitoring and assessment of control performance for single loop systems. Industrial & Engineering Chemistry Research, 41(5): 1297-1309. http://dx.doi.org/10.1021/ie0101285

[17] Cockram, T.J., Lautieri, S.R. (2007). Combining security and safety principles in practice. Institution of Engineering and Technology International Conference on System Safety, pp. 159-164. http://dx.doi.org/10.1049/cp:20070458

[18] Yang, W., Zhao, Q. (2014). Cyber security issues of critical components for industrial control system. Proceedings of 2014 IEEE Chinese Guidance, Navigation and Control Conference, Yantai, pp. 2698-2703. https://doi.org/10.1109/CGNCC.2014.7007593

[19] Aissa, A.B., Abercrombie, R.K., Sheldon, F.T., Mili, A. (2010). Quantifying security threats and their potential impacts: A case study. Innovations in Systems and Software Engineering, 6(4): 269-281. https://doi.org/10.1007/s11334-010-0123-2

[20] Caswell, J. (2011). Survey of Industrial Control Systems Security. Washington University in St. Louis, St. Loius, Missouri.

[21] Hildick-Smith, A. (2005). Security for critical infrastructure SCADA systems. SANS GSEC Practical Assignment, Version 1.4c, Option 1, February 23, 2005.

[22] Vulnerability analysis of energy delivery control system. Idaho National Laboratory, Idaho Falls INL/EXT-10-18381, September 2011.
[23] Amin, S., Crdenas, A., Sastry, S.S. (2009). Safe and secure networked control systems under denial-of-service attacks. Hybrid Systems: Computation and Control, 31-45. http://dx.doi.org/10.1007%2f978-3-642-00602-9_3
[24] Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H. (2012). SCADA security in the light of Cyber Warfare. Computers & Security, 31(4): 418-436. https://doi.org/10.1016/j.cose.2012.02.009
[25] Stouffer, K., Falco, J., Scarfone, K. (2011). Guide to industrial control systems (ICS) security. National Institute of Standards and Technology (NIST), Gaithersburg, MD Special Publication, 800-82.
[26] Onyeji, I., Bazilian, M., Bronk, C. (2014). Cyber security and critical energy infrastructure. The Electricity Journal, 27(2): 52-60. https://doi.org/10.1016/j.tej.2014.01.011
[27] Sheldon, F.T., Abercrombie, R.K., Mili, A. (2008). Evaluating security controls based on key performance indicators and stakeholder mission. 4th Workshop on Cyber Security and Information Intelligence Research (CSIIRW'08), Oak Ridge, Tennessee, pp. 1-11.