INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, e-ISSN 1841-9844, 14(3), 419-436, June 2019.

Reliability Assessment Model for Industrial Control System Based on Belief Rule Base

Y.H. Wang, P.L. Qiao, Z.Y. Luo, G.L. Sun, G.Z. Wang

Yuhe Wang, Peili Qiao*, Zhiyong Luo, Guanglu Sun, Guangze Wang
School of Computer Science and Technology
Harbin University of Science and Technology
Harbin 150080, China
*Corresponding author: qiaopl@hrbust.edu.cn

Guangze Wang
Library
Harbin University of Science and Technology
Harbin 150080, China

Abstract: This paper establishes a novel reliability assessment method for industrial control system (ICS). Firstly, the qualitative and quantitative information were integrated by evidential reasoning(ER) rule. Then, an ICS reliability assessment model was constructed based on belief rule base (BRB). In this way, both expert experience and historical data were fully utilized in the assessment. The model consists of two parts, a fault assessment model and a security assessment model. In addition, the initial parameters were optimized by covariance matrix adaptation evolution strategy (CMA-ES) algorithm, making the proposed model in line with the actual situation. Finally, the proposed model was compared with two other popular prediction methods through case study. The results show that the proposed method is reliable, efficient and accurate, laying a solid basis for reliability assessment of complex ICSs.

Keywords: Belief rule base (BRB), industrial control system (ICS), evidential reasoning (ER), reliability assessment, covariance matrix adaptation evolution strategy (CMA-ES) algorithm.

1 Introduction

The industrial control system (ICS) integrates computer technology, communication and the control theory [9]. It is widely used in infrastructure industries like power transmission, water supply, oil and gas transportation, etc. In the ICS, each controller regulates multiple components. The fault or intrusion of one component will threaten the security of the entire system. Once the ICS fails, the user will not only lose monitoring and control, but also suffer from facility damage, economic losses and even casualties. Therefore, it is of great significance to accurately assess the reliability of the ICS, especially in complex applications [12].

The existing ICS reliability assessment methods are mainly based on knowledge, model or data [18]. The knowledge-based methods include fault mode, effects, and criticality analysis (FMECA) [10], fault tree [8], decision tree [1], and risk analysis [15]. These approaches mainly rely on qualitative or quantitative knowledge. The model-based methods, namely, open-switch fault diagnosis [20], signal-based coding [11] and processing fault diagnosis [12], can diagnose the faults of different systems according to the actual industrial processes. However, it is difficult to build effective models for large-scale ICSs. The data-based methods emerge due to the proliferation of industrial data collection techniques, such as distributed control system (DCS) and supervisory control and data acquisition (SCADA). Relying on historic process data, many data-based methods are suitable for ICS fault detection, e.g. Shewhart individuals control chart [5], Hotelling's T-squared (T^2) control chart [2], quality control chart [17], principal component analysis (PCA) [16], and knowledge discovery in databases (KDD) [19].

Copyright ©2019 CC BY-NC

Each type of the above methods has its defects. For knowledge-based methods, the experts are often unable to obtain the accurate qualitative knowledge, owing to the complexity of the ICS and the numerous factors [13]. The model-based methods depend heavily on specific samples and cannot be extended easily to general cases. Neither can they use qualitative or quantitative data. The data-driven methods work well in reliability assessment of accurate data samples, but perform poorly in differentiating normal data from abnormal data [14]. What is worse, the ICS data cannot be acquired under certain conditions. To sum up, the existing methods cannot effectively utilize all the various uncertain information in the ICS, including expert knowledge and historical data. It is imperative to develop an approach to assess ICS reliability against these semi-quantitative data.

To solve the above problems, this paper integrates qualitative and quantitative information by evidential reasoning (ER) rule, and then establishes an ICS reliability assessment model based on belief rule base (BRB), which is a powerful nonlinear strategy for uncertainty problems [6] [22]. In this way, both expert experience and historical data were fully utilized in the assessment. Finally, the initial parameters were optimized by covariance matrix adaptation evolution strategy (CMA-ES) algorithm, making the proposed model in line with the actual situation [7].

The remainder of this paper is organized as follows: Section 2 analyzes the reliability of the ICS; Section 3 sets up a BRB-based model and applies it to assess the ICS reliability; Section 4 compares the proposed model with two other methods through a case study on a tobacco factory; Section 5 wraps up this paper with several meaningful conclusions.

2 Problem overview

2.1 ICS structure

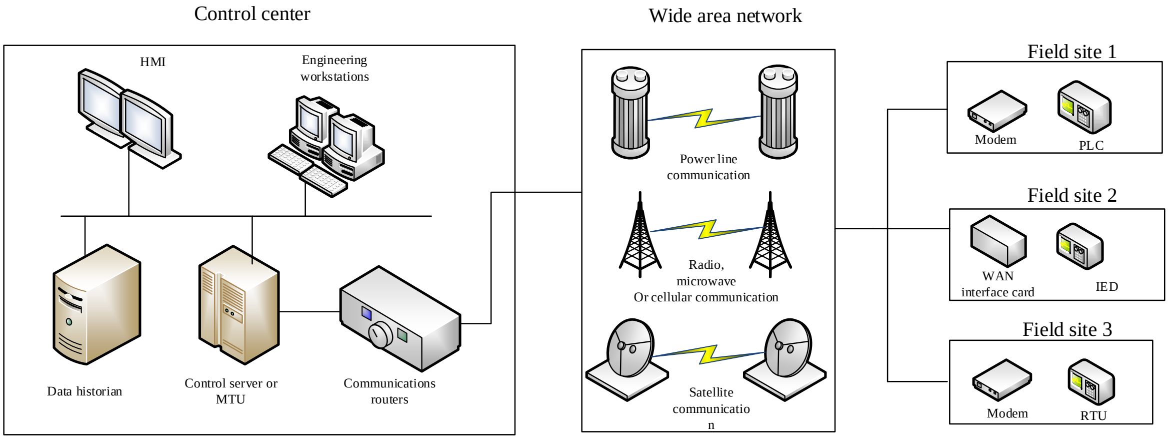

Figure 1: Typical SCADA structure

Consider SCADA as a typical ICS, the structure of SCADA is illustrated in Figure 1 [21]. In the control center, there are a human-machine interface (HMI), an engineering workstation, a data historian, a master terminal unit (MTU) and a communication router. All these components are connected via a local area network (LAN). Among them, the HMI mainly displays the data collected from the site, while the MTU stores and processes input and output data. In the wide area network, the information is transmitted between the control center and the field sites via power line, radio, microwave, cellular or satellite. On the field sites, there are multiple distributed remote terminal units (RTUs) or programmable logic controllers (PLCs), which control local processes. The ICS can collect various data, analyze the trend and issue alarms when parameters exceed the allowable range.

According to the struture of SCADA, the main components of ICS can be divided into three types as shown in Table 1 [3].

Table 1: The type of main components in ICS

First level	Second level	Third level
ICS components	Hardware components	PLC
		RTU
		HMI
		MTU
		Other hardware
	Software components	OS(Operation system)
		DB(Data base)
		Software of SCADA system
		Software of PLC
		Other software
	Communication	Profinet
		Communication routers
		Modem
		Other communication components

2.2 The framework for ICS reliability assessment

The accuracy of ICS reliability assessment hinges on the clear identification of various influencing factors. In fact, these factors can be divided into internal factors and external factors. As shown in Table 1, the internal factors are the faults of the system components, including software fault, hardware fault and communication fault, while the external factors include network attacks and human errors, both of which directly bears on the system security. Therefore, the ICS reliability can be assessed from both the fault and security of the system.

On this basis, the framework of ICS reliability assessment was constructed. As shown in Figure 3, the framework consists of three layers: the target layer, the criteria layer and the plan layer. The target layer is the reliability assessment; the criteria layer encompasses fault assessment and security assessment; the plan layer contains various antecedent attributes that affect the criteria layer.

2.3 Process of ICS reliability assessment

Firstly, the fault and security attributes of the ICS were integrated by the ER rule for fault and security analyses. Based on the analysis results, the BRB was adopted to establish a model and CMA-ES for training. Finally, the ICS reliability assessment model was obtained. The specific steps are presented in Figure 4 below.

2.4 Mathematical description

Let FA, SC and FR be the fault assessment result, security assessment result and final result of ICS reliability assessment, respectively. The set of antecedent attributes C^1 and that C^2 for fault assessment and security assessment can be respectively expressed as:

$$C^1 = \left\{c_1^1, c_2^1, \cdots c_n^1\right\} \tag{1}$$

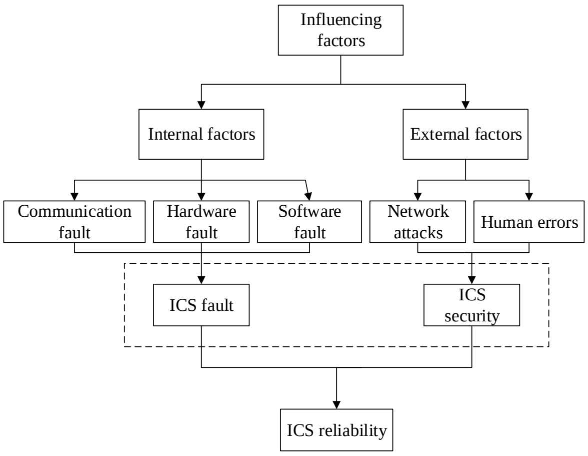

Figure 2: Relationship between influencing factors and ICS reliability

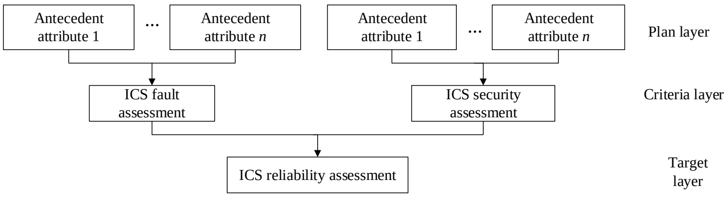

Figure 3: Framework of ICS reliability assessment

$$C^2 = \left\{c_1^2, c_2^2, \cdots c_m^2\right\} \tag{2}$$

where c_i^1 and c_i^2 are the i-th antecedent attribute for fault assessment and security assessment, respectively.

Then, the fault assessment result and security assessment result can be respectively obtained by:

$$FA = ER_1\left(C^1, t^1\right) \tag{3}$$

$$SC = ER_2\left(C^2, t^2\right) \tag{4}$$

where $ER_1(\bullet)$ is the relationship between the leading attribute and the fault assessment result; t^1 is the set of parameters for $ER_1(\bullet)$; $ER_2(\bullet)$ is the relationship between the leading attribute and the security assessment result; t^2 is the parameters of $ER_2(\bullet)$. On this basis, the BRB-based ICS reliability assessment result can be obtained by combining the fault and security assessment results:

$$FR = BRB(FA, SC, t) \tag{5}$$

where $BRB(\bullet)$ is the conversion from fault and security assessment results to reliability assessment result; t is a set of parameters.

3 Construction of BRB-based ICS reliability assessment model

As mentioned before, the first step of ICS reliability assessment is to clearly identify all the faults in the system components. After all, the fault of one component will threaten the security of the entire system. Moreover, the ICS reliability assessment must consider both quantitative data (e.g. system duration, fault frequency and PLC fault tolerance) and qualitative data (e.g.

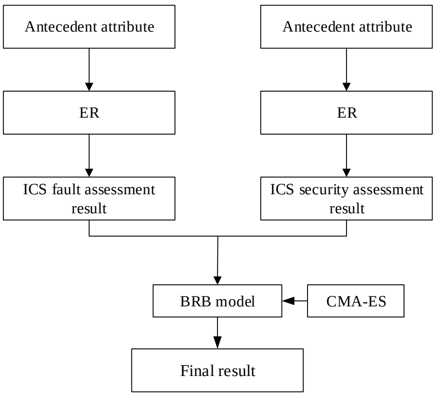

Figure 4: The process of ICS reliability assessment

terminal controllability, communication stability). The former can be collected by data monitoring system, while the latter require expert interpretation. If the two types of data are uncertain, it is impossible to assess the ICS reliability in an accurate manner.

Considering the excellent performance of the ER and the BRB for uncertainty problems, the author decided to set up a multi-layer ICS reliability assessment model, optimize the model with the historical data of the BRB, and integrate multiple attributes with the ER rule. The proposed model contains a fault assessment model and a security assessment model. Besides, the parameters was trained by the CMA-ES algorithm, such that the assessment indices are in line with the actual situation.

3.1 Fault assessment attributes

Reliability is defined as the ability or possibility to perform a specified function without failure within a specified time and under specified conditions. The reliability of the system can be evaluated by mean time to repair, failure rate and mean time to failure [22].

In our framework of ICS reliability assessment, the fault assessment covers three aspects. For each attribute, the weight t is the most important parameter in the ER process. The antecedent attributes of fault assessment are listed in Table 2.

3.2 Security assessment attributes

The ICS security is partially affected by network attacks. The common attacks include virus and trojan attack, DoS attack, detection attack, U2R attacks and R2L attack. Specifically, the virus and trojan attack destroys the ICS or steals system data with a malicious program; the DoS consumes an excessive amount of ICS resources, making services unavailable; the detection attack scans the ICS network and unlocks the hidden security dangers; the U2R attack acquires the rights of the ICS superuser through manipulation of the ICS vulnerabilities; the R2L attack remotely gains unauthorized access to the ICS. The different attacks pose varied levels of threats and brings diverse damages to the ICS. Therefore, the attack type, continuous attack time, attack frequency and attack severity were selected as the antecedent attributes of the security assessment.

The ICS security is also affected by human errors like mis-operation, unauthorized entry, etc. Hence, the occurrence frequency and severity of such errors were also taken as the antecedent attributes of the security assessment. Table 3 lists all the antecedent attributes of the security assessment.

Table 2: The antecedent attributes of fault assessment

First level	**Second level**	**Third level**
The Fault Reliability of ICS	Hardware Reliability of ICS	The Rate of Failure $(c_{11}^1)(t_{11}^1 = 0.15)$
		MTTF(Mean Time to Failure $(c_{12}^1)(t_{12}^1 = 0.2)$
		MTTR(Mean Time to Repair) $(c_{13}^1)(t_{13}^1 = 0.15)$
		MPMT(Mean Preventive Maintenance Time) $(c_{14}^1)(t_{14}^1 = 0.1)$
		MPBF(MeanTime Between Failure) $(c_{15}^1)(t_{15}^1 = 0.1)$
		The Failure Severity $(c_{16}^1)(t_{16}^1 = 0.15)$
		The Failure Tolerance $(c_{17}^1)(t_{17}^1 = 0.15)$
	Software Reliability of ICS$(c_2^1)(t_2 = 0.15)$	MTTF(Mean Time to Failure) $(c_{21}^1)(t_2^1 = 0.2)$
		MTTR(Mean Time to Repair) $(c_{22}^1)(t_{22}^1 = 0.2)$
		The Fluency of Software $(c_{23}^1)(t_{23}^1 = 0.3)$
		MPBF(Mean Time Between Failure) $(c_{24}^1)(t_{24}^1 = 0.15)$
		The Rate of Failure $(c_{25}^1)(t_{25}^1 = 0.15)$
	Communication Reliability of ICS	The Rate of Lost $(c_{31}^1)(t_{31}^1 = 0.2)$
		The Packet Loss Rate $(c_{32}^1)(t_{32}^1 = 0.3)$
		MTTF(Mean Time to Failure) $(c_{33}^1)(t_{33}^1 = 0.2)$
		The Failure Severity $(c_{34}^1)(t_{34}^1 = 0.2)$
		Delay rate $(c_{35}^1)(t_{35}^1 = 0.15)$

3.3 ER rule process

ER rule is developed as a multi-criteria decision analysis (MCDA) approach on the basis of belief decision and D-S theory [22]. Compared to the D-S theory of evidence, the calculation process of the ER rule is linear. The ER rule can be implemented in the following steps:

Assume that there are P basic attributes $\{c_1, \cdots c_i, \cdots c_P\}$ of a general attribute C in a two-level hierarchy, and $\{t_1, \cdots, t_i, \cdots t_p\}$ denotes the weights of the basic attributes, where $0 \leq t_i \leq 1$. There are M assessment grades.

Step 1. Convert the belief of each assessment level into belief. The conversion is shown in

Table 3: The antecedent attributes of security assessment

First level	Second level	Third level	Forth level
The Security Reliability of ICS(CS)	Security Event (c_1^2)($t_1^2 = 0.5$)	The type of attacks (c_{11}^2)$c_{11}^2 = 0.2$)	Virus and trojan attack (c_{111}^2)($t_{111}^2 = 0.3$)
			U2R attacks (c_{112}^2)($c_{112}^2 = 0.2$)
			R2L attack (c_{113}^2)($c_{113}^2 = 0.2$)
			Dos attack (c_{114}^2)($c_{114}^2 = 0.3$)
		Continuous attack time (c_{12}^2)($t_{12}^2 = 0.2$)	
		The frequcy of attacks (c_{13}^2)($t_{13}^2 = 0.3$)	
		The Severity of attacks (c_{14}^2)($t_{14}^2 = 0.3$)	
	Error Operatio (c_2^2)($t_2^2 = 0.5$)	The Rate of events (c_{21}^2)($t_{21}^2 = 0.5$)	
		The Severity of attacks (c_{22}^2)($t_{22}^2 = 0.5$)	

Figure 5, where $Q_{i,j}$ represents the basic probabilistic set relative to the j-th assessment level $Q_{i,\Theta}$ is the rest of probabilistic set of the unassigned to any resultaccording to the i-th attribute, $\overline{Q_{i,\Theta}}$ denotes unallocated basic probability mass relative to the in significant degree of the i-th basic attribute, $Q_{i,\Theta}$ represents the unassigned basic probability mass with respect to the incompleteness of the i-th basic attribute.

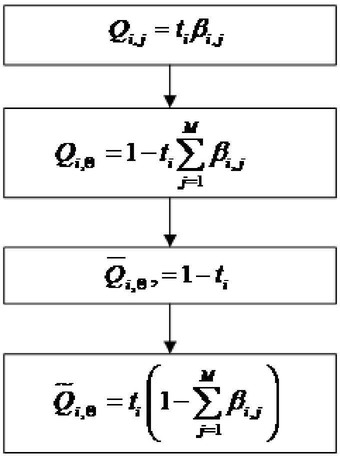
$Q_{i,j} = t_i\beta_{i,j}$
$Q_{i,\Theta} = 1 - t_i\sum_{j=1}^{M}\beta_{i,j}$
$\bar{Q}_{i,\Theta}, = 1 - t_i$
$\tilde{Q}_{i,\Theta} = t_i\left(1 - \sum_{j=1}^{M}\beta_{i,j}\right)$

Figure 5: The conversion process

Step 2. Combine the first i-th attributes through the ER, and the detailed process can be describe as Figure 6.

where $Q_{I(i+1),j}$ represents the probability set of the j-th evaluation grade after the combi-

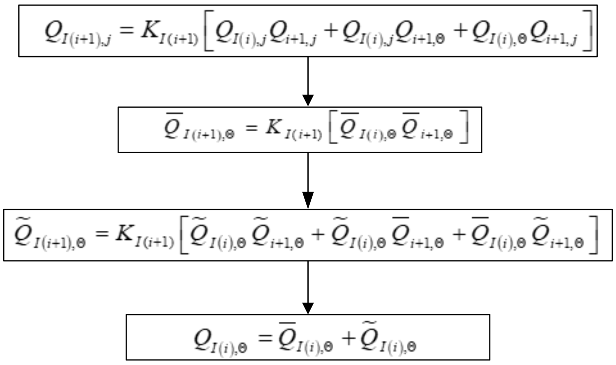
$Q_{I(i+1),j} = K_{I(i+1)}\left[Q_{I(i),j}Q_{i+1,j} + Q_{I(i),j}Q_{i+1,\Theta} + Q_{I(i),\Theta}Q_{i+1,j}\right]$
$\overline{Q}_{I(i+1),\Theta} = K_{I(i+1)}\left[\overline{Q}_{I(i),\Theta}\overline{Q}_{i+1,\Theta}\right]$
$\widetilde{Q}_{I(i+1),\Theta} = K_{I(i+1)}\left[\widetilde{Q}_{I(i),\Theta}\widetilde{Q}_{i+1,\Theta} + \widetilde{Q}_{I(i),\Theta}\overline{Q}_{i+1,\Theta} + \overline{Q}_{I(i),\Theta}\widetilde{Q}_{i+1,\Theta}\right]$
$Q_{I(i),\Theta} = \overline{Q}_{I(i),\Theta} + \widetilde{Q}_{I(i),\Theta}$

Figure 6: The combination process

nation of the first i-th basic attributes, and $K_{I(i+1)}$ can be calculated by:

$$K_{I(i+1)} = \frac{1}{1 - \sum_{k=1}^{N}\sum_{\substack{j=1\\j\neq k}}^{N} P_{I(i),k}P_{i+1,j}} \tag{6}$$

Step 3. Determine the belief of the j-th assessment level and the belief of the unassigned attributes by:

$$\widehat{\beta}_j = \frac{Q_{I(M),j}}{1 - \overline{Q}_{I(M),\Theta}} \quad (j = 1, 2, \cdots, N) \tag{7}$$

$$\widehat{\beta}_\Theta = \frac{\widetilde{Q}_{I(M),\Theta}}{1 - \overline{Q}_{I(M)\Theta}} \tag{8}$$

Compute the belief of the assessment results after determining all attributes:

$$\begin{array}{l} \beta_{i,j} = \frac{C_{i,j+1} - U(c_i)}{C_{i,j+1} - C_{i,j}} \left(C_{i,j+1} \leq U\left(c_i\right) \leq C_{i,j+1}\right) \\ \beta_{i,j+1} = 1 - \beta_{i,j} \\ \beta_{i,k} = 0 (k = 1, \cdots, N, k \neq j, j+1) \end{array} \tag{9}$$

where $U\left(c_i\right)$ is the value of attribute c_i and $c_{i,j}$ is the j-th reference value of c_i .

The ER rule can be described as an attribute fusion process. Based on the original data on the ICS, the various attributes should be mixed and then partially allocated to the third layer. Then, the assessment level of second layer attributes should be determined according to the third layer attributes, and that of first layer attributes according to the second layer attributes. Finally, the attributes of the three layers were integrated again by the ER rule, yielding to final ICS assessment result.

3.4 The reliability model based on BRB

The assessment results fused by ER rule should be graded according to the safety assessment result and fault assessment result, because the ICS reliability is an integration of fault and security. Then, the fused results will be taken as the input of the BRB model. As shown in Table 4, there are five reliability levels in FA and SC :

$$C^1 \in \{TW, B, G, E, TB\} \tag{10}$$

Table 4: Reliability level for ICS

Reliability Level	**The level of fault assessment (FA)**	**The level of security assessment (SC)**	**The level of Final result (FR)**
1(The worst)	TW	TW	TW
2(Bad)	B	B	B
3(Good)	G	G	G
4(Excellent)	E	E	E
5(The best)	TB	TB	TB

$$C^2 \in \{TW, B, G, E, TB\} \tag{11}$$

where C^1 is the reliability level of FA ; C^2 is the reliability level for of SC . The final result FR can be described as:

$$FR = (FR_1, FR_2, FR_3, FR_4, FR_5) = (\{TW, B, G, E, TB\}) \tag{12}$$

The reliability of R_k can be expressed as:

if $FA = C_k^1$ and $SC = C_k^2$, then $FR = \{(SC_1, t_{1,k}), \cdots, (SC_5, t_{5,k})\}$ with a rule weight θ_k and attribute weights ρ_{c^1} and ρ_{c^2} .

The BRB model have 25 rules in the initial case. The initial belief of the rules was determined by reliability assessment. If the fault assessment or security assessment are the worst (TW), it is impossible to guarantee the data accuracy in the ICS, i.e. the assessment result must the worst (TW). For example, the reliabilities of R_5, R_{10} , R_{15} , R_{20} , R_{25} can be expressed as:

$$\begin{array}{l} IfFAisTWandSCisTW, theFRis\{(TW,1),(B,0),(G,0),(E,0),(TB,0)\} \\ IfFAisBandSCisTW, theFRis\{(TW,1),(B,0),(G,0),(E,0),(TB,0)\} \\ IfFAisGandSCisTW, theFRis\{(TW,1),(B,0),(G,0),(E,0),(TB,0)\} \\ IfFAisEandSCisTW, theFRis\{(TW,1),(B,0),(G,0),(E,0),(TB,0)\} \\ IfFAisTBandSCisTW, theFRis\{(TW,1),(B,0),(G,0),(E,0),(TB,0)\} \end{array} \tag{13}$$

3.5 The reasoning process of BRB model

To obtain the stability of the ICS, the BRB model was derived by the ER method through the following steps:

Step 1. Calculate the matching degree of the antecedent attribute of the training sample to a rule:

$$a_i^k = \begin{cases} \dfrac{A_i^{l+1} - a_i(t)}{A_i^{l+1} - A_i^l} & k = l \\ \dfrac{a_i(t) - A_i^l}{A^{l+1} - A_i^l} & k = l + 1 \\ 0 & k = 1, \cdots, K(k \neq l, l+1) \end{cases} \tag{14}$$

where a_i^k is the i-thantecedent rule; $a_i(t)$ is the i-th attribute in the data; A_i^l and A_i^{l+1} are the reference value of the l-th and ($l + 1$) - thantecedent attributes, respectively; k represents the number of belief rules.

Step 2. Compute the weight of the k-th rule from the matching degree t_i^k :

$$t_k = \frac{\theta_k \prod_{i=1}^{M} \left(a_i^k\right)^{\overline{\delta}_i}}{\sum_{l=1}^{K} \theta_l \prod_{i=1}^{M} \left(a_i^l\right)^{\overline{\delta}_i}} \tag{15}$$

where $\overline{\rho}_i$ is the i-thantecedent attribute.

Step 3. Integrate the rules and generate belief of different outputs by the analytic synthesis algorithm of the ER which was described in Chapter 3.3.

Step 4. Generate the final output according to the belief of different outputs:

$$FA_{actual} = \sum_{n=1}^{N} C_n t_n \tag{16}$$

3.6 CMA-ES optimization of the BRB

The BRB was optimized under following three constraints: rule weight, attribute weight and rule. The rule weight constraint, reflecting the relative importance of the rule, can be expressed as:

$$0 \leq \theta_k \leq 1, \quad k = 1, 2, \ldots L \tag{17}$$

The attribute weight must be normalized to [0, 1]:

$$0 \leq \rho_n \leq 1, n = 1, \ldots, T_k \tag{18}$$

Similarly, the rule must be normalized to [0, 1]:

$$0 \leq \rho_n \leq 1, n = 1, \ldots, T_k \tag{19}$$

where $t_{i,k}$ is the belief of the k-th rule. The value of $t_{i,k}$=1 if the modified rule can be fully executed and smaller than one if otherwise:

$$\sum_{i=1}^{N} t_{i,k} \leq 1, \quad k = 1, 2, \ldots, L \tag{20}$$

$$output_{estimated} = \sum_{n=1}^{N} p\left(SC_i\right) t_i \tag{21}$$

Next, the BRB parameters should be trained by the objective function to reduce the error between the assessed and actual outputs. Here, the error is measured by the mean square error (MSE):

$$\operatorname{MSE}\left(\theta_k, t_{i,k}, \rho_n\right) = \frac{1}{T} \sum_{i=1}^{T} \left(\text{ output }_{\text{estimated}} - \text{ output }_{\text{actual}}\right)^2 \tag{22}$$

The objective function and constraints of the BRB parameter training can be expressed as:

$$\begin{aligned} & \min \operatorname{MSE}\left(\theta_k, t_{i,k}, \rho_n\right) \\ & 0 \leq \theta_k \leq 1 \\ & 0 \leq \rho_n \leq 1, n = 1, \ldots, T_k \\ & 0 \leq t_{i,k} \leq 1, \quad i = 1, \ldots, N, \quad k = 1, 2, \ldots L \\ & \textstyle\sum_{i=1}^{N} t_{i,k} \leq 1 \end{aligned} \tag{23}$$

The parameter training with the L-CMA-ES consists of four steps:

Step 1. Parameter initialization. The initial $mean^0$ is equal to the initial parameter Ω^0,and Ω is:

$$\Omega = \{\theta_1, \ldots, \theta_L, \beta_{1,\cdots}, \ldots, \beta_{N,}, \delta_1, \ldots, \delta_{T_k}\} \tag{24}$$

where the initial value of each parameter is given by the expert.

Step 2. Population sampling. Taking the central solution as the central expectation of the solution space, a normal distribution population is generated as:

$$\Omega_q^{g+1} \sim mean^g + \eta^g \mathbb{N}\left(0, \mathbf{C}^g\right)(q = 1, \cdots, n) \tag{25}$$

where Ω^0 is the first solution in the solution space; $\Omega_q^{g+1}$is the q-th solution in the solution space, g is the number of iterations; $mean$ is the mean distribution, i.e. the central expectation; η is the step size; C is the covariance matrix of the population.

Step 3. Selection and recombination. The candidate solution in the solution space are screened by leaky bucket mechanism. After the candidate solutions satisfying the constraints are obtained, the solutions of the child populations will be selected in the population according to the adaptive function. Then, the central expectation in the population moves towards the local optimal solution, and guides the evolution of the population. When the previous optimal solution population ε is obtained, the population's expectations can be updated by:

$$mean^{g+1} = \sum_{i=1}^{\varepsilon} \gamma_i \Omega_{i,\mu}^{g+1} \left(\sum_{i=1}^{\varepsilon} \gamma_i = 1\right) \tag{26}$$

where ε is the number of child populations; γ is individual weight (the total weight is 1); μ is the size of the parent population; $\Omega_{i:\mu}$ means the i-th candidate solution is obtained from the parent population μ in the $(g+1)$-th iteration according to the fitness value.

After recombination, the central region of the population will move towards the child populations, such that the candidate solution is more accurate than the parent population.

Step 4. Update of covariance matrix. In the next iteration, the optimal solution needs to be found based on the covariance matrix. During the iteration process, the transformation of the covariance matrix varies with the length and orientation of the long axis of the elliptical distribution of the population. The change in orientation reflects the trend and direction of evolution, while the change in length represents the scope of the population search. The covariance matrix should be updated by:

$$\mathbf{C}^{g+1} = \left(1 - a_1 - a_\varepsilon\right)\mathbf{C}^g + a_1 p^{g+1}\left(p^{g+1}\right)^T + a_\varepsilon \sum_{i=1}^{\varepsilon} \gamma_i \left(\frac{\left(\Omega_{i,\mu}^{g+1} - mean^g\right)}{\eta^g}\right)\left(\frac{\left(\Omega_{i,\mu}^{g+1} - mean^g\right)}{\eta^g}\right)^T \tag{27}$$

where a_i and a_ε is the total learning rate; p is the evolution path (initial value=0). Then, the evolution path should be updated as:

$$p^{g+1} = \left(1 - a_p\right)p^g + \sqrt{a_p\left(2 - a_p\right)\left(\sum_{i=1}^{s} \gamma_i^2\right)^{-1}} \frac{mean^{g+1} - mean^g}{\eta^g} \tag{28}$$

where $a_p \leq 1$ is the retrospective period of the evolution path. The step η should be updated as:

$$\eta^{g+1} = \eta^g \exp\left(\frac{a_\eta}{d_\eta}\left(\frac{\left|\left|p_\eta^{g+1}\right|\right|}{\mathrm{E}||\mathbb{N}(0, \mathbf{I})||} - 1\right)\right) \tag{29}$$

where d_η is the damping coefficient; $\mathrm{E}||\mathrm{N}(0, \mathrm{I})||$ is the expectation of the Euclidean paradigm $||N(0, \mathbf{I})||$; I is the vector of the unit matrix; $a_\eta$is the look back window; p_η is the conjugate evolution path (initial value=0). The conjugate evolution path should be updated as:

$$p_{\eta}^{g+1} = (1 - a_{\eta}) p_{\eta}^{g} + \sqrt{a_{\eta} (2 - a_{\eta}) \left(\sum_{i=1}^{\varepsilon} \gamma_i^2 \right)^{-1}} \mathbf{C}^{(g)-\frac{1}{2}} \frac{m^{g+1} - m^{g}}{\eta^{g}} \tag{30}$$

The above formula(27-30) should be executed repeatedly until reaching the accuracy requirement. Then, the optimal solution should be outputted, and serve as the model inputs after training.

4 Case study

4.1 The assessment grades of the attributes

Since the ICS reliability is affected by external and internal factors, this section designs simulation experiments involving both internal faults and external security incidents. The experiments were carried out in the actual industrial control environment. The faults and incidents were selected and rated empirically by experts. Some of them are quantitative information, and some are qualitative. Both internal faults and external security incidents were divided into four levels according to the actual situation (Table 5). The dataset was derived from the log events of a Chinese tobacco factory, which were recorded over 100 days by a PLC-controlled device in SCADA system.

Table 5: The levels of internal faults

	Worst	**Bad**	**Good**	**Best**
c_{11}^{1}(times/day)	15	10	5	0
c_{12}^{1}(hours)	3	12	21	30
c_{13}^{1}(minutes)	60	40	20	10
c_{14}^{1}(minutes)	(minutes)	60	40	20
c_{15}^{1}(hours)	3	12	21	30
c_{16}^{1}	Given by Experts			
c_{17}^{1}	Given by Experts			
c_{21}^{1}(hour)	3	12	21	30
c_{22}^{1}(minutes)	1	40min	20min	10
c_{23}^{1}	Given by Experts			
c_{24}^{1}(hour)	3	12	21	30
c_{31}^{1}(times/ day)	5	3	1	0
c_{32}^{1}(%)	10	5	3	0%
c_{33}^{1}(hour)	10	20	30	40
c_{34}^{1}	Given by Experts			
c_{35}^{1}(seconds)	1s	0.3s	0.1s	0.01s

4.2 Internal and external reliabilities based on ER rule

The original data were fused by the ER algorithm, using the attributes and reference levels in Table 5-6. The fusion follows the process detailed in Section 3. According to the ER algorithm, the author obtained quantitative observation data for 30 days, which reflect the internal reliability of the ICS. The daily observation data are shown in Figure 7. It can be seen from Figure 7 that the internal reliability of the ICS fluctuated violently, indicating a high frequency of system faults, while the external reliability changed less significantly, which reflects the moderate frequency of external attacks.

Table 6: The levels of external security incidents

	Worst	Bad	Good	Best
c^2_{111}	Given by Experts			
c^2_{112}	Given by Experts			
c^2_{113}	Given by Experts			
c^2_{114}	Given by Experts			
c^2_{12}(minutes)	20	10	5	0
c^2_{13}(times/day)	5	3	1	0
c^2_{14}	Given by Experts			
c^2_{21}(times/day)	5	3	1	0
c^2_{22}	Given by Experts			

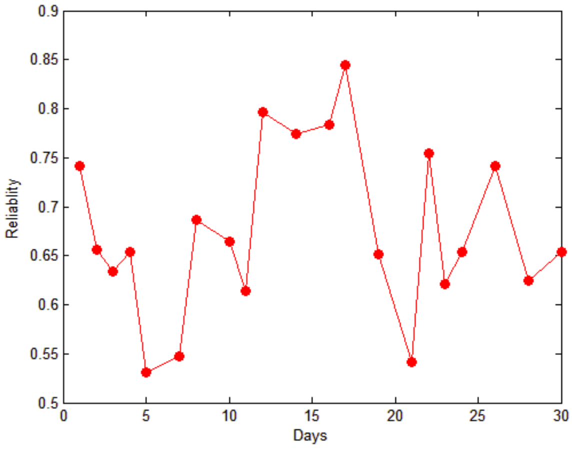

Figure 7: Internal reliabilities for 30 days

4.3 Model construction

The proposed method (BRB) was contrasted with two prediction models, i.e. back propagation neural network (BP) and Markov prediction model (MM). For consistency, the initial parameters of all three methods were trained by the CMA-ES algorithm. The BP is a popular data-based prediction model. This model takes Gaussian functions as training neurons, and adopts radial basis function kernels in the middle layer for nonlinear transform of input parameters. Compared with traditional neural networks, the BP enjoys a small scale and fast operation, thanks to the limited number of intermediate layers.

The MM is a typical semi-quantitative assessment model based on bayesian decision theory. It bears high resemblance to the proposed BRB model. The high accuracy and efficiency have earned it immense popularity.

The initial weights and levels of belief rules are listed in Table 7. The initial parameters of the two contrastive algorithms are given in Table 8. The input parameters of the CMA-ES

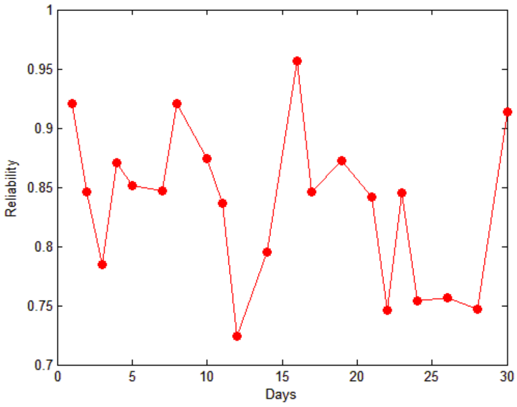

Figure 8: External reliabilities for 30 days

Table 7: Initial weights and levels of belief rules

Rule	**Rule Weight**	**SC(t)**	**SC1, SC2, SC3, SC4, SC5=TW, B, G, E, TB**
1	1	TW	$(SC_1,1),(SC_2,0),(SC_3,0),(SC_4,0),(SC_5,0),(SC,0)$
2	1	B	$(SC_1,0),(SC_2,1),(SC_3,0),(SC_4,0),(SC_5,0),(S,0)$
3	1	G	$(SC_1,0),(SC_2,0),(SC_3,1),(SC_4,0),(SC_5,0),(SC,0)$
4	1	E	$(SC_1,0),(SC_2,0),(SC_3,0),(SC_4,1),(SC_5,0),(SC,0)$
5	1	TB	$(SC_1,0),(SC_2,0),(SC_3,0),(SC_4,0),(SC_5,1),(S,0)$

Table 8: The initial parameters of the two contrastive methods

Comparison	**Initial parameters**
MM	Initial probability vector = [0.2,0.2,0.2,0.2,0.2];
	Initial probability transition matrix = [1,0,0,0,0;0,1,0,0,0;0,0,1,0,0;0,0,0,1,0;0,0,0,0,1];
BP	Input neuron: 3;Output neuron: 1;
	Sliding window size: 3

Table 9: The input parameters of the CMA-ES algorithm

The semantic	**Initial parameters**
value	$m^0 = O^0$; $\sigma^0 = 0.5; \lambda = 13$; $\tau = 6$; $a_1 = 0.0031$; $a_\tau = 0.0066$; $p_\psi^0 = 0$; $a_\psi = 0.147$; $p_\sigma^0 = 0$; $a_\sigma = 0.1813$; $d_\sigma = 1.1813$; $e = 0.6$; Loop = 100;

algorithm are displayed in Table 9.

4.4 Simulation and result analysis

Ten rounds of validations were performed to verify the effectiveness of our method. The exact range of the result was determined through interval estimation.The 100 reliability values

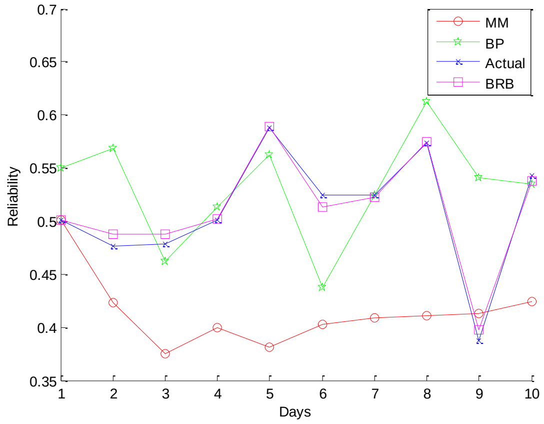

Figure 9: The results of round 1

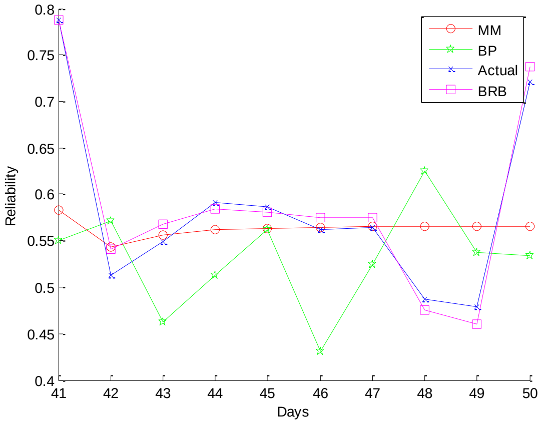

Figure 10: The results of round 5

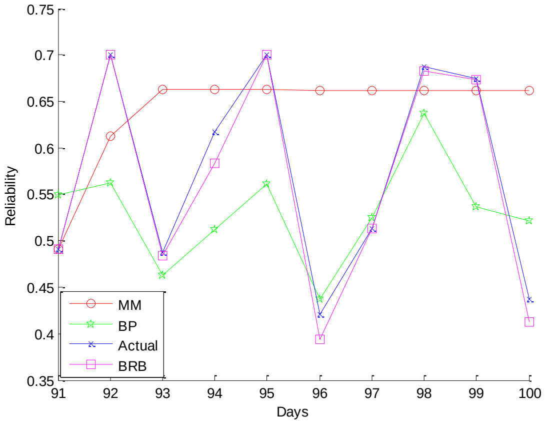

Figure 11: The results of round 10

were divided into 10 groups. The first 9 groups were adopted as the training data, and the rest as the test data. The results of the first, fifth and tenth round of training are presented in Figure 9, 10 and 11, respectively.

Table 10: The MSEs after round 10

Rounds	**1**	**2**	**3**	**4**	**5**
BRB	$4.676e^{-5}$	$3.097e^{-5}$	$1.345e^{-4}$	$0.987e^{-4}$	$1.362e^{-4}$
MM	$0.963e^{-2}$	$6.698e^{-3}$	$2.322e^{-2}$	$6.342e^{-2}$	$3.987e^{-2}$
BP	$2.547e^{-3}$	$3.147e^{-3}$	$6.357e^{-3}$	$7.214e^{-3}$	$1.365e^{-2}$
Rounds	**6**	**7**	**8**	**9**	**10**
BRB	$7.321e^{-4}$	$8.541e^{-5}$	$1.247e^{-4}$	$6.218e^{-5}$	$1.361e^{-4}$
MM	$0.897e^{-2}$	$3.657e^{-3}$	$3.465e^{-2}$	$7.645e^{-2}$	$1.644e^{-2}$
BP	$1.247e^{-2}$	$4.365e^{-3}$	$4.514e^{-3}$	$5.987e^{-3}$	$7.365e^{-3}$

Table 10 lists the MSEs between the predicted results and the actual results of the three methods after round 10.

Table 11 provides the overall MSEs and the interval estimation results of the three methods after round 10. The interval estimation results refer to the mean estimation interval at the confidence level of 95%.

Table 11: The results of overall MSEs and the interval estimation after round 10

	MSE	**Interval estimation (95%)**
BRB	2.36 e^{-4}	[2.12 e^{-4}, 3.87 e^{-4}]
MM	2.16 e^{-4}	[1.37 e^{-2}, 3.98 e^{-2}]
BP	6.37 e^{-3}	[3.780 e^{-3}, 8.98 e^{-3}]

The above results show that the proposed BRB model, the MM and the BP respectively controlled the MSE on the order of 1,000th, 100th and 1,000th. Thus, our model reduced the error by 100 times from the level of the MM. Moreover, our model achieved a small and acceptable error range. Thus, the proposed method is reliable and efficient, in addition to its good prediction accuracy.

5 Conclusions

Considering the internal and external influencing factors of ICS reliability, this paper puts forward a new ICS reliability assessment model based on the BRB. The ICS reliability assessment was divided into internal fault assessment and external security assessment, making the assessment more objective. The BRB can process semi-quantitative information in our samples, which contain both quantitative data and qualitative knowledge. In this way, the model can be trained well with sufficient samples. The initial training parameters were optimized by the CMA-ES algorithm, aiming to improve the accuracy of model inputs. Finally, the proposed model was compared with two other popular prediction methods through case study. The results show that the proposed method is reliable, efficient and accurate, laying a solid basis for reliability assessment of complex ICSs.

Funding

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

Author contributions. Conflict of interest

The authors contributed equally to this work. The authors declare no conflict of interest.

Bibliography

[1] Alambeigi, F.; Wang, Z.; Hegeman, R. (2019). Autonomous data-driven manipulation of unknown anisotropic deformable tissues using unmodelled continuum manipulators, *IEEE Robotics and Automation Letters*, 4(2), 254-261, 2019.

[2] Brereton, R. G. (2016). Hotelling's T squared distribution, its relationship to the F distribution and its use in multivariate space, *Journal of Chemometrics*, 30(1), 18-21, 2016.

[3] 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 and Soft Computing Research*, 5(3), 205-220, 2015.

[4] Franco, I. C.; Schmitz, J. E.; Costa, T. V. (2017). Development of a predictive control based on Takagi-Sugeno model applied in a nonlinear system of industrial refrigeration, *Chemical Engineering Communications*, 204(1), 39-54, 2017.

[5] Goedhart, R.; Schoonhoven, M.; Ronald, J. M. M. (2016). Correction factors for Shewhart and control charts to achieve desired unconditional ARL, *International Journal of Production Research*, 54(24), 7464-7479, 2016.

[6] He, W.; Hu, G. Y.; Zhou, Z. J. (2018). A new hierarchical belief-rule-based method for reliability evaluation of wireless sensor network, *Microelectronics Reliability*, 87, 33-51, 2018.

[7] Hu, G. Y.; Zhou, Z. J.; Zhang B. C. (2016). A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm, *Applied Soft Computing*, 48(C), 404-418, 2016.

[8] Jin, L. J.; Peng, C. Y.; Jiang, T. (2017). System-level electric field exposure assessment by the fault tree analysis, *IEEE Transactions on Electromagnetic Compatibility*, 59(4), 1095-1102, 2017.

[9] Kriaa, S.; Pietre, L.; Bouissou, M. (2015). A survey of approaches combining safety and security for industrial control systems, *Reliability Engineering & System Safety*, 139, 156-178, 2015.

[10] Lee, Y. S.; Kim, D. J.; Kim, J. O. (2011). New FMECA methodology using structural importance and fuzzy theory, *IEEE Transactions on Power Systems*, 26(4), 2364-2370, 2011.

[11] Liu, Z.; Liu, T.; Han, J. (2017). Signal model-based fault coding for diagnostics and prognostics of analog electronic circuits, *IEEE Transactions on Industrial Electronics*, PP(99), 1-1, 2017.

[12] Luo, Z. Y.; Wang, P.; You, B. (2016). Serial reduction optimization research of complex product workflow's accuracy under the time constraint, *Advances in Mechanical Engineering*, 8(10), 1-9, 2016.

[13] Luo, Z. Y.; You, B.; Liu, J. H. (2016). Research of the intrusion tolerance state transition system based on semi-markov, *Transactions of Beijing Institute of Technology*, 36(7), 712-717, 2016.

[14] Luo, Z. Y.; You, B.; Xu, Z. B. (2014). Automatic recognition model of intrusive intention based on three layers attack graph, *Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)*, 44(5), 1392-1397, 2014.

[15] Navarro, A. D.; Yip, H. M.; Wang, Z. (2016). Automatic 3-d manipulation of soft objects by robotic arms with an adaptive deformation model, *IEEE Transactions on Robotics*, 32(2), 429-441, 2016.

[16] Pacella, M. (2018). Unsupervised classification of multichannel profile data using PCA: An application to an emission control system, *Computers & Industrial Engineering*, 122, 161-169, 2018.

[17] Rusmini, P.; Crippa, V.; Cristofani, R. (2016). The role of the protein quality control system in SBMA, *Journal of Molecular Neuroscience*, 58(3), 348-364, 2016.

[18] Sang, W.; Livne, E. (2016). Probabilistic aeroservoelastic reliability assessment considering control system component uncertainty, *Aiaa Journal*, 54(8), 2507-2520, 2016.

[19] Thomas, M. C.; Zhu, W.; Romagnoli, J. A. (2017). Data mining and clustering in chemical process databases for monitoring and knowledge discovery, *Journal of Process Control*, S095915241730032X, 2017.

[20] Wang, Z.; Li, P.; Navarro, A. D. (2015). Design and control of a novel multi-state compliant safe joint for robotic surgery, *IEEE International Conference on Robotics and Automation (ICRA)*, 1023-1028, 2015.

[21] Wang, Z.; Yip, H. M.; Navarro, A. D. (2016). Design of a novel compliant safe robot joint with multiple working states, *IEEE/ASME Transactions on Mechatronics*, 21(2), 1193-1198, 2016.

[22] Zhou, Z. J.; Hu, G. Y.; Zhou, Z. J. (2017). A Model for hidden behavior prediction of complex systems based on belief rule base and power set, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, PP(99), 1-7, 2017.