sensors

MDPI

Article

A Three-Stage Dynamic Assessment Framework for Industrial Control System Security Based on a Method of W-HMM

Xudong Ji, Hongxing Wei, Youdong Chen *, Xiao-Fang Ji and Guo Wu

School of Mechanical Engineering and Automation, Beihang University, Beijing 100191, China; jixd@buaa.edu.cn (X.J.); weihongxing@buaa.edu.cn (H.W.); xiaofangji163@163.com (X.-F.J.); wuguobeijing@buaa.edu.cn (G.W.)

* Correspondence: chenyd@buaa.edu.cn

Abstract: Industrial control systems (ICS) are applied in many fields. Due to the development of cloud computing, artificial intelligence, and big data analysis inducing more cyberattacks, ICS always suffers from the risks. If the risks occur during system operations, corporate capital is endangered. It is crucial to assess the security of ICS dynamically. This paper proposes a dynamic assessment framework for industrial control system security (DAF-ICSS) based on machine learning and takes an industrial robot system as an example. The framework conducts security assessment from qualitative and quantitative perspectives, combining three assessment phases: static identification, dynamic monitoring, and security assessment. During the evaluation, we propose a weighted Hidden Markov Model (W-HMM) to dynamically establish the system's security model with the algorithm of Baum–Welch. To verify the effectiveness of DAF-ICSS, we have compared it with two assessment methods to assess industrial robot security. The comparison result shows that the proposed DAF-ICSS can provide a more accurate assessment. The assessment reflects the system's security state in a timely and intuitive manner. In addition, it can be used to analyze the security impact caused by the unknown types of ICS attacks since it infers the security state based on the explicit state of the system.

Keywords: security; dynamic assessment; industrial control systems; weighted hidden Markov model

Citation: Ji, X.; Wei, H.; Chen, Y.; Ji, X.-F.; Wu, G. A Three-Stage Dynamic Assessment Framework for Industrial Control System Security Based on a Method of W-HMM. *Sensors* **2022**, *22*, 2593. https://doi.org/10.3390/s22072593

Academic Editors: Savio Sciancalepore, Giuseppe Piro and Nicola Zannone

Received: 4 March 2022
Accepted: 25 March 2022
Published: 28 March 2022

1. Introduction

The industrial control system can be remotely interacted with and communicated with cloud services [1], cyber-physical systems [2], or edge devices in a highly networked environment [3]. Cyber-attacks are increasingly becoming a threat to ICS; thus, their security is critical [4,5]. Once an essential piece of equipment experiences a safety incident, it causes a shutdown of the system and even causes casualties [6].

The security assessment of industrial control systems is an integral part of security [7,8]. The system's security integrates internal attributes and external environments. The elements involved in assessment have the following characteristics: large number, strong correlation, and poor accessibility. Thus, evaluating the security of the system accurately is difficult.

In recent years, security assessment research has mainly focused on artificial intelligence [9], medical subjects [10,11], infrastructure [12], power systems [13], coal mining [14], chemicals [15], etc. The industrial field focuses on assessing the system's functional safety or the static information security assessment for the design, and its security status is easily observerd [16,17]. However, the critical equipment executing complex control tasks in ICS is challenging for capturing security statuses directly. System security information is also related to running variables, such as system operating status and environmental status. Security assessment must have the ability to obtain security information of complex systems dynamically.

New cyberattacks for which its forms and types tend to be unknown are hard to be detected [18]. Due to the limited resources of devices and networks in ICS [19,20], it

is hard to obtain security information of assessments directly by detecting attacks [21]. Cyberattacks make ICS more undependable and unsafe when using the Internet [22]. Scholars generally evaluate system security through the consequences of information attacks [23]. Consequence refers to the property losses caused by an information attack. For example, Muhammad Adil et al. identified a jamming attack channel by detecting different transmission frequencies and Round Trip Time (RTT) of transmitting a signal from multi-channel in WSNs transmission media [24].

There are three methods of assessment based on consequences of attacks [20,25]: qualitative assessment, quantitative assessment [26], and the combination of them. There are many qualitative evaluation methods, such as attack trees and fuzzy calculations. These methods are coarse-grained assessments of system parameters. For example, Xu Hui et al. used attack trees to identify various attacks for security management of SDN [27]. However, they could not provide a quantitative value to evaluate the consequences of the attack. The quantitative evaluation methods can assess the impacts of information attacks. Wenli Shang et al. provided a security assessment method based on an attack tree model with fuzzy set theory and probability risk assessment technology [28]. Jingjing Hu et al. proposed a multi-dimensional network security risk assessment framework [29], including two stages: risk identification and risk calculation. They used HMM to assess the network security risk in the risk calculation stage. The HMM assessment method can effectively reflect and quantify the security risks of the physical network system. However, they did not assign the weight to the result in the risk value calculation, as the network servers and nodes have different importance. We should weigh different parts of ICS in ICS due to its heterogeneity. Nary Subramanian et al. proposed a quantitative method of NFR (non-functional requirements) safety assessment for the infrastructure system of oil pipeline systems [30]. This method can solve the integrated assessment of functional safety and security. However, it cannot calculate the assessed value of the security. Aziz A. et al. used ontology knowledge to analyze the causal relationship between events [31], established corresponding probability models, and identified the consequences of abnormalities. This method can quantitatively assess the consequences of the system's attacks. However, the probability established by this method was stationary, while the system risk is changing. It is challenging to apply dynamic evaluations.

Currently, the most commonly used security assessment method is a combination of qualitative and quantitative information [32,33]. One is the analytic hierarchy process, which is a multi-level weight decision analysis method. Jun Chen applied the analytical hierarchy process for industrial control system evaluation [34]. Moreover, it can effectively evaluate industrial control risks. However, it cannot dynamically assess the system of ICS due to unknown attacks and threats that follow ICS. Some pieces of research had brought focus onto the necessity of a framework for the evaluation of IoT device security [35,36]. The above research methods are not dynamic and cannot meet this assessment requirement.

We propose a practical security assessment framework, a three-stage dynamic assessment framework for ICS based on a method of W-HMM. The main contributions of this work are as follows:

i. The proposed method combines a qualitative and quantitative assessment of ICS security dynamically by using a W-HMM model. The method can infer the system's risk value, which can be used as a system risk reference in a timely and intuitive manner through the explicit consequences of the attack on the device.
ii. The assessment of the industrial robot control system (IRCS) is used as an example to illustrate the use of the method and compared with two typical security assessment methods.

The article is structured as follows. In the next section, we introduce the static recognition of DAF-ICSS. Dynamic monitoring is described in Section 3. Section 4 shows the assessment. Section 5 explains the framework of DAF-ICSS. Section 6 uses an IRCS as an example to verify DAF-ICSS. We discuss the results in Section 7. Finally, Section 8 summarizes the work of this paper.

2. Static Recognition

2.1. Basic Value

The ICS is a part of the company's fixed assets, and its security will affect the value of the company's fixed assets. We use the analytic hierarchy process to evaluate the basic value of ICS. The basic value, B_v, is used to assess the economic value of ICS. The basic value is divided into three layers: target layer, factor layer, and index layer, shown in Figure 1.

The target layer obtains B_v. The factor layer decomposes the basic value of the ICS into two critical factors: asset value and asset status. Asset value represents the economic value of the ICS, and asset status reflects the state and the environment. The index layer decomposes the factors into the fine-grained index. The asset value includes three values: self-value S_v, indirect value A_v, and accident value A_c. Self-value refers to the asset value of the ICS. Indirect value is the indirect economic loss of the enterprise caused by ICS failure without injury. accident value represents the estimated financial loss of an injury accident caused by ICS attacks. It is obtained from accident probability f_1 and accident loss g.

$$A_c = f_1 \times g \tag{1}$$

Asset status is divided into three states: self-state h, network state N_s, and work environment E_s, as shown in Table 1. The self-state reflects the performance and stability of the system, thereby affecting asset value. The latter two reflect the harshness of the system's external environment and affect the system's vulnerability value. Network state refers to the value determined by the network bandwidth, traffic, and peak value. The working environment is the value determined by temperature, humidity, and electromagnetic interference. The smaller the valuation, the lower the risk. The basic value is calculated as follows.

$$B_v = S_v \times h + A_v + A_c \tag{2}$$

Table 1. Quantitative table of asset status.

State	Description	Valuation
Self-state h	No-fault, available	0.25
	Fault-fixed, warning	0.5
	Fault but not affecting the main function, dangerous	0.8
Network state N_s	Network bandwidth utilization $\leq$ 50%, steady flow	0.5
	Network bandwidth utilization $\leq$ 80%, flow fluctuation	1
	Network bandwidth utilization $\geq$ 80%, flow fluctuates greatly	1.5
Work environment E_s	Temperature normal, Humidity drying, Weak electromagnetic interference	0.5
	One item is out of rating	0.8

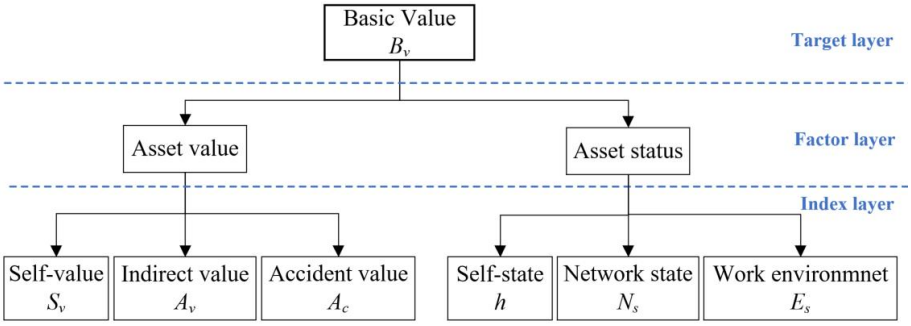

Figure 1. The basic value decomposition diagram.

2.2. Vulnerability

The vulnerability V_v of ICS refers to the system's weakness that attackers can abstract [37]. When the vulnerability of an ICS is attacked, a basic attack path model should be shown in Figure 2. The attack is achieved through three steps: network path connection, data manipulation, and breaking through protection. The first step ensures that the attacker can connect to ICS through the network. The second step is that the attacker sends malicious attack instructions when the attacker could imitate external communication data of ICS. The third step hides or floods attack instructions so that the instructions can pass through the protection. The attack instructions could steal, change, or delete the system's data. Moreover, the attack may cause the system's faults.

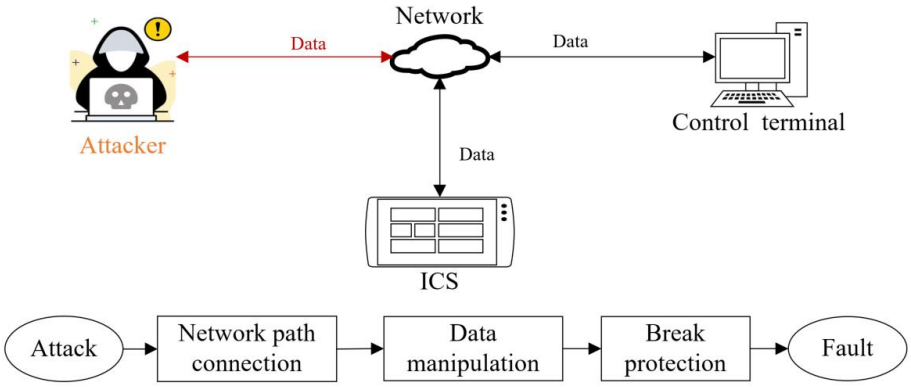

Figure 2. The processes of the attack path model.

The vulnerability of ICS can be illustrated from three factors depending on the three steps of the attack path model. The three factors are availability A_a, data weakness S_r, and safety protection S_w. Availability means the degree that ICS can achieve specific operations through the network when random attacks are launched. Data weakness evaluates the possibility of communication data being attacked. Security protection is the system's ability to prevent information attacks. These three factors respectively assess the vulnerability of the three steps of the attack model. Figure 3 shows the hierarchy diagram of vulnerabilities of ICS.

$$A_a = l \times m \times r \tag{3}$$

$$S_r = log_2(2^v + 2^u + 2^w) \tag{4}$$

$$S_w = C_p \times S_p \times F_r \tag{5}$$

The availability is divided into three indexes to measure the difficulty of attackers connecting to the system: Vector l, complexity m, and authentication r. l is used to measure the network distance between the attacker and ICS. Before an attacker can connect to the system, he must transfer instructions through network nodes such as routing equipment. The more nodes are, the more inefficiently the instructions connect. m describes the level of attack method that an attacker can achieve. When the attacker is connected to the system, r will be an index to stop the connection. The description and corresponding valuation, which are given by experts of cybersecurity, are shown in Table 2.

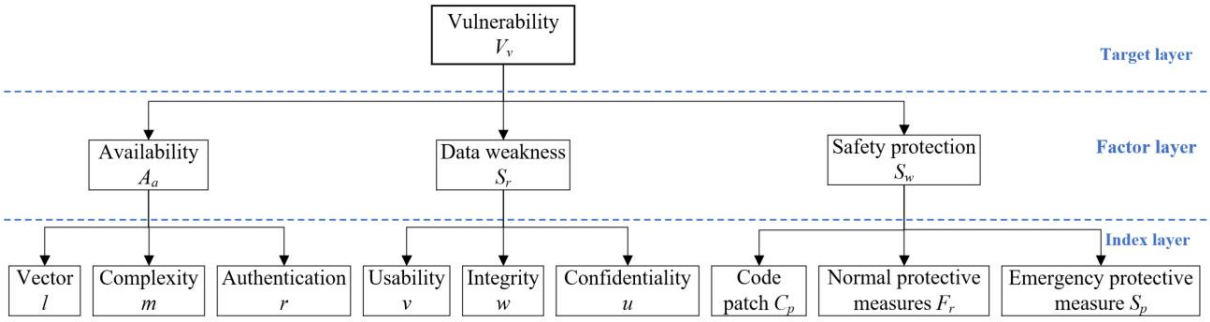

Figure 3. Hierarchy diagram of the vulnerability of ICS.

Table 2. The valuation of availability.

	Description	Valuation
Vector l	Remote	0.85
	Neighbor	0.62
	Local	0.55
	Port physical connection	0.2
Complexity m	Primary	0.71
	Secondary	0.61
	Senior	0.35
Authentication r	Repeatedly	0.45
	Single	0.56
	None	0.704

The data weakness is divided into three indexes: confidentiality u, integrity w, and usability v, as shown in Table 3.

Table 3. Data weakness valuation value.

	Description	Valuation
Usability v	Process parameters viewing commands	0.2
	System parameters viewing commands	0.3
	All parameters viewing commands	0.4
	Process parameters editing commands	0.6
	System parameters editing commands	0.8
	All parameters editing commands	1
Integrity w	Syntax verification audit	0.7
	Pre and post content verification audit	0.5
	Hazard verification audit	0.3
Confidentiality u	Encryption	0.3
	Unencrypted, nonstandard	0.5
	Unencrypted, standard	0.9

Safety protection S_w includes three indexes: code patch C_p, normal protective measure F_r, and emergency protective measure S_p, shown in Table 4. Code patch reflects the extent of the patches covering system vulnerabilities. Normal protective measure refers to the ability to protect the system against information attacks under normal operating conditions. The emergency protective measure is the capability to handle emergencies when in danger. The vulnerability value V_v is shown as follows.

$$V_v = N_s \times (2 \times A_a + S_r + S_w)/3 \quad (6)$$

Table 4. Safety protection value.

	Description	Valuation
Code patch C_p	All	0.1
	Part	0.4
	None	0.7
Normal protective measure F_r	More than two	0.2
	One or two	0.6
	None	0.9
Emergency protective measure S_p	Soft response (without damaging the equipment under the premise of safety)	0.3
	Hard reaction (equipment May be damaged when ensuring safety)	0.5
	None	0.8

3. Dynamic Monitoring

3.1. W-HMM Establishment

The HMM model can be used to build a dynamic evaluation model. Describing the stochastic process of generating explicit state sequences from hidden state sequences, HMM is a probability model related to time series. Each hidden state generates an explicit state. The security status of ICS is mostly unobservable. All the operations and the faults caused by the attack are recorded in the system's log. The security is related to the fault with a certain observation probability. The probability of mutual transition between security states is the occurrence probability. By using the occurrence probability of the security state, the current system risk probability can be calculated to monitor the system's risk dynamically.

However, HMM cannot distinguish the magnitude of the danger caused by different states. This paper proposes a W-HMM (weight HMM) method. W-HMM is the optimization method of HMM and weighs the results calculated by HMM. The value of weight is estimated based on the magnitude of the danger. The aim is to improve the accuracy of the evaluation when calculating the risk value. In W-HMM, we optimize the calculation of HMM results by weighing the security state. The W-HMM model is proposed, shown in Figure 4.

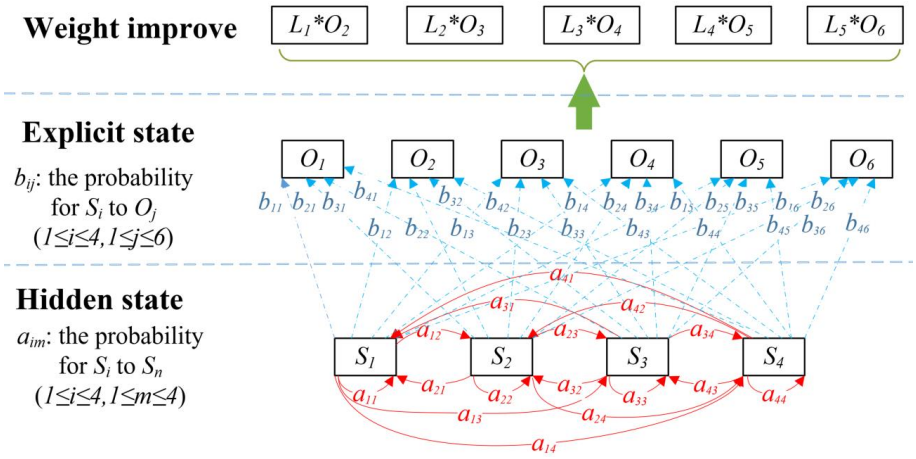

Figure 4. The W-HMM model.

We construct a mapping relation of the Markov process with parameters. The security state can be categorized into secure S_1, monitored S_2, attacked S_3, and captured S_4 states. S_2 indicates that the system is scanned or spied by an attacker. In this state, the bandwidth resources are occupied, and parameters will be stolen. In the attacked state, the attacker sends malicious data, but the system has not been captured. In the captured

state, the system is captured by the attacker to execute the attacker's instructions. In this state, the system may crash or perform dangerous operations. According to the severity of the fault, system faults are classified into normal O_1, error O_2, mild alarm O_3, and warning O_4; moderate alarm O_5; and serious alarm O_6, as shown in Figure 5 and Table 5.

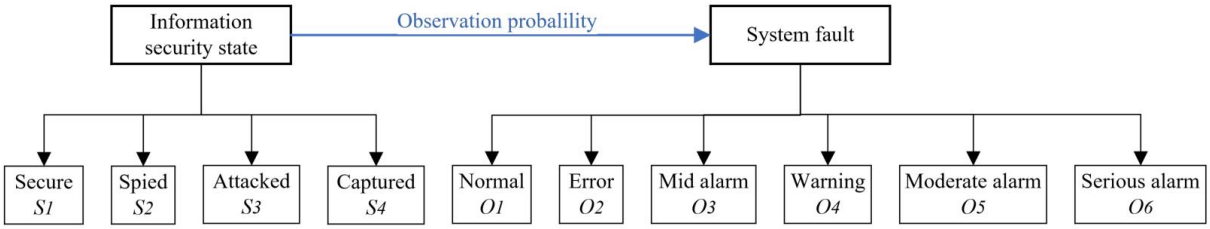

Figure 5. The analysis diagram of security and system fault.

Table 5. Example of system faults.

System Faults	Identifier	Example
Normal	O_1	/
Error	O_2	Program syntax error, user password error, etc.
Mild alarm	O_3	The planning path may exceed The limit of the system, etc.
Warning	O_4	System acceleration approaching the setting threshold, etc.
Moderate alarm	O_5	Speed exceeds the threshold during running, then alarm and stop running, etc.
Serious alarm	O_6	The system detects motor overcurrent, then alarm and emergency stop, etc.

3.2. Calculating Occurrence Probability of Security by W-HMM

The specific steps are as follows.

1. Constructing State and Model

The explicit state set O and the hidden state set S are, respectively, shown as follows.

$$O = O_j(1 \le j \le 6) \tag{7}$$

$$S = S_i(1 \le i \le 4) \tag{8}$$

The development relationships between hidden states is related by $a_{im}(1 \le i, m \le 4)$. a_{im} is the probability of transition from state S_i at time t to state S_m at time $t+1$.

The hidden state is represented by the explicit state. $b_{ij}(1 \le i \le 4, 1 \le j \le 6)$ is called the explicit state probability matrix, and shows the relationship between hidden and explicit state. b_{ij} is the probability of transition from the state S_i at time t to state O_j at the time $t+1$.

The state transition probability matrix A and the explicit state probability matrix B can be written as follows.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \tag{9}$$

$a_{im} = P(x_{t+1} = S_m \mid x_t = S_i)$, $1 \le m \le 4, 1 \le i \le 4$

$$B = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} \\ b_{31} & b_{32} & b_{33} & b_{34} & b_{35} & b_{36} \\ b_{41} & b_{42} & b_{43} & b_{44} & b_{45} & b_{46} \end{bmatrix} \tag{10}$$

$b_{ij} = P(x_{t+1} = O_j \mid x_t = S_i)$, $1 \le j \le 6, 1 \le i \le 4$

The W-HMM of the ICS can be described as λ, among which π represents the probability of the initial state, which is shown as follows.

$$\lambda = (A, B, \pi)$$
$$where\ \pi = P(x_i = S_i),\ \ 1 \le i \le 4 \tag{11}$$

2. Algorithm of Baum–Welch

Markov model correction algorithms based on state sequences are classified into supervised and unsupervised learning algorithms [38]. A supervised learning algorithm records a large amount of state data to estimate the parameters. However, it is time consuming, costly, and causes difficulty in evaluating parameters dynamically. Unsupervised learning algorithms identify model parameters based on training samples and are suitable for calculating the parameters of W-HMM of ICS. To accurately describe the system and adapt to system changes, the W-HMM model is trained and updated iteratively with the Baum–Welch algorithm [39]. It is possible to obtain (see Appendix A) Equation (12), which represents the W-HMM model after $n+1$ iterations. When adding new sample data, the current Markov parameters are taken as the initial parameters, and Baum–Welch iterative calculations are carried out to obtain the latest parameters. The occurrence probability of security risks is extracted from the state transition probability matrix of parameters.

$$\lambda^{n+1} = \left(A^{n+1}, B^{n+1}, \pi^{n+1}\right) \tag{12}$$

4. Assessment

Field experts of ICS obtained the state weight values that affect the risk value of ICS, shown in Table 6. The risk value describes the loss caused by an attack on the company. It is equal to the product of the failure probability and consequence of the attack. The security risk value can be determined as follows.

$$SV = E_s \times B_v \times e^{V_v} \times \left\{ L_1 \times \sum_{n=2}^{n=4} \left(\pi^{n+1}(i) \times b_{i2}\right) + \cdots + L_5 \times \sum_{n=2}^{n=4} \left(\pi^{n+1}(i) \times b_{i6}\right) \right\} \tag{13}$$

From Equation (13), L_1, L_2, L_3, L_4, and L_5 are the weight values of the five states in the observation states (O_2, O_3, O_4, O_5, and O_6). Since some model parameters change with time, they are classified according to the measurement of their period, demonstrated in Table 7.

Table 6. State weight value.

	Weight
L_1	0.5
L_2	1
L_3	2
L_4	2.5
L_5	4

Table 7. Type of parameters.

Type	**Identifier**	**Description**
Constant	$L_1 - L_5$	It only needs to be collected once and can be used for a long time
	V_v	
	A_c	
	A_v	

Table 7. *Cont.*

Type	Identifier	Description
Stage constant	E_s	Regular collection and evaluation are required
	S_v	
	h	
Real-time volume	SV	Real-time acquisition and calculation
	π	
	B	

5. Framework of DFA-ICSS

Illustrated in Figure 6, the DAF-ICSS framework is composed of static identification, dynamic monitoring, and evaluation. The framework can evaluate the security of ICS qualitatively and quantitatively. In this section, we will briefly summarize the procedure of the assessment.

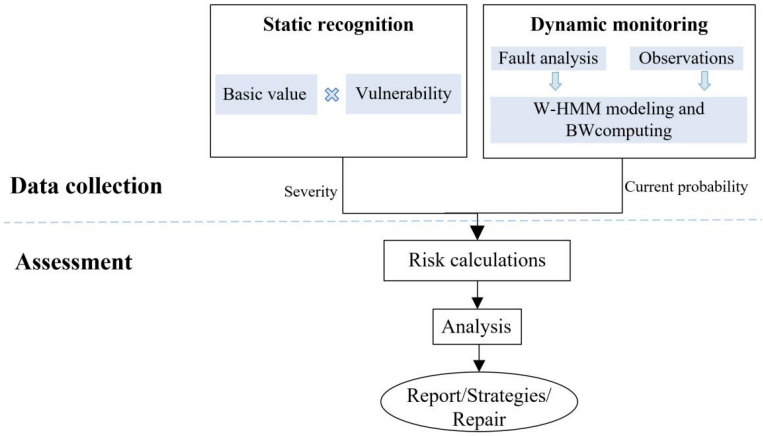

Figure 6. Security evaluation framework of DAF-ICSS.

During data collection, there are two stages. One is static identification, which identifies the value and vulnerability of each part of the evaluation system. The analytic hierarchy process enumerates the factors that affect the value and the vulnerability of the system. The result of static identification is represented by a severity value, which is obtained by multiplying the value and vulnerability of the system.

The other is dynamic monitoring, which calculates the system's security risk probability. Moreover, the calculation is based on W-HMM. Its result predicts the possibility of system security risks.

The system security state is unobservable. W-HMM is introduced for dynamic monitoring to establish the connection between the observable states and the unobservable security state. This method calculates the risk probability according to the observation state and updates the risk probability in the next new observation state. W-HMM can quantify and weigh the risk probability based on different application scenarios and models.

In the assessment stage, we obtain the system risk value by multiplying the severity value and the risk probability. We develop a risk map. The map determines the risk level by the risk value's boundary. The boundary is set by the risk tolerance of the system, shown in Figure 7. The system is safe when the risk value is in the green area. If it is in the yellow area, the system is at risk. The evaluation system will immediately issue an alarm if it reaches the red zone. Its purpose is to locate risk levels according to the calculated risk value quickly. The corresponding protection strategy can be chosen rapidly according to the level and risk value.

Figure 7. Risk map.

6. Experiments and Results

6.1. Experimental Setup

An attack test platform is built to verify the feasibility and effectiveness of the evaluation method proposed in this paper, shown in Figure 8.

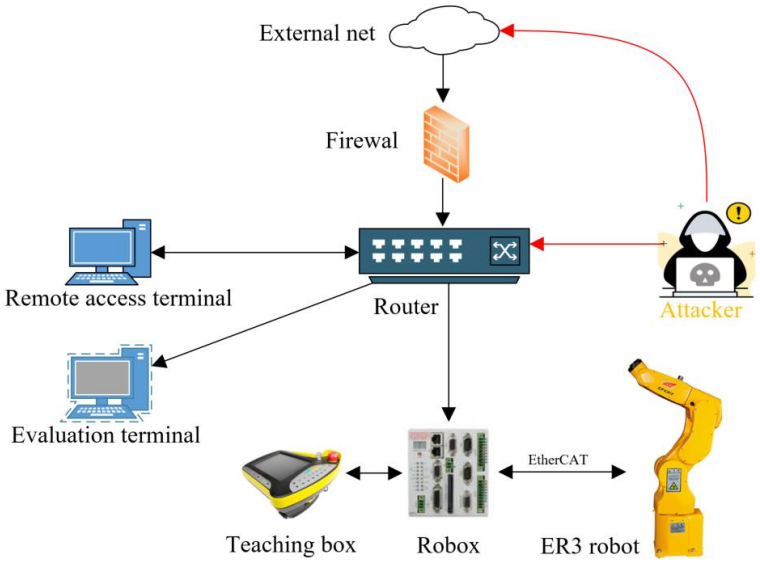

Figure 8. The topography of the system.

The platform comprises three computers and a robot that are connected through a gigabit router. The robot, which is ER3, is produced by Effort. The controller of the robot is Robox produced by Robox SPA.

The computers play as the remote terminal, the evaluation terminal, and the attack terminal. The remote terminal sends instructions and programs. The attack terminal attacks the control system. Meanwhile, the evaluation terminal records the robot's status data and evaluates the system.

6.2. Experimental Data Collection and Calculation

- Step 1: Static identification

The company's asset data and data evaluated by asset management are shown in Table 8. Table 9 displays the vector and complexity in availability. When the robot connects to the PC, the robot does not perform authentications or check the content of the communication. As a result, the authentication score is 0.704. Most system security measures are warnings. The valuation of data weakness can be found in Table 9. Most system faults are alarming. When a serious failure occurs, the system will stop running. The score of the emergency protective measure is 0.5.

- Step 2: Dynamic monitoring

The initial parameters of the model are obtained by collecting and sorting empirical data. The initial parameters A^0, B^0, and π^0 are obtained by empirical estimation. We used two types of DOS attacks during the experiment in the two periods. In the first period, the hacker uses ping flooding random attacks. In the second period, the hacker uses UDP attacks to attack the vulnerable spots of the system. In the experiment, the attacked ports are random, and the attack frequency is once every 10 min.

- Step 3: Assessment

The failure of the industrial control system caused by the attack is probabilistic. We divide the experiment into two stages. Each attack stage lasts a week, and the robot control system status is collected once an hour during the working time every day. We record the status of the control system with three different methods: DAF-ICSS, expert [40] and HMM [41]. The data obtained by these methods are shown in Table 10. We obtain the average value of each stage evaluation from the on-site enterprise expert group.

Table 8. Basic value datasheet of the robot unit.

Property	Name	Identifier	Valuation	Remarks
Self-value S_v	Controller, sensors and accessories, etc.	/	CNY 40,000	Collection of financial information
Indirect value A_v	Labor, equipment, product lost, etc,	/	CNY 160,000	
Accident value A_c	Accident probability	f_1	0.01	Statistics
	Accident loss	g	CNY 1,000,000	
Asset status	Self-state	h	0.25	Query the above related assessment form after evaluation
	Network state	N_s	1.5	
	Work environment	E_s	0.8	

Table 9. Control system information sheet.

Property	Name	Identifier	Valuation	Remarks
Availability A_a	Vector	l	0.55	Check the evaluation form according to the information
	Complexity	m	0.61	
	Authentication	r	0.704	
Data weakness S_r	Usability	v	0.5	
	Integrity	w	0.7	
	Confidentiality	u	0.5	
Safety protection S_w	Code patch	C_p	0.7	
	Normal protective measure	F_r	0.9	
	Emergency protective measure	S_p	0.5	

Table 10. The data of the observation sequence.

Stage 1				
Day	Observation sequence	Expert (CNY 10^4)	HMM (CNY 10^4)	DAF-ICSS (CNY 10^4)
Day 1	$O_1, O_1, O_1, O_1, O_1, O_2, O_1, O_4$	1.60	1.75649	1.7498
Day 2	$O_1, O_1, O_1, O_3, O_1, O_3, O_2, O_4$		2.17419	2.51482
Day 3	$O_1, O_3, O_1, O_2, O_1, O_4, O_1, O_5$		2.27618	2.79187
Day 4	$O_1, O_1, O_1, O_2, O_1, O_5, O_1, O_5$		2.0854	2.72481
Day 5	$O_1, O_1, O_1, O_1, O_2, O_3, O_2, O_6$		2.04967	2.66117
Day 6	$O_1, O_2, O_1, O_3, O_1, O_6, O_2, O_4$		2.13676	2.86088
Day 7	$O_2, O_1, O_3, O_1, O_4, O_4, O_5, O_6$		2.2158	2.92729

Table 10. *Cont.*

Stage 2				
Day 1	$O_1, O_5, O_2, O_6, O_2, O_4, O_4, O_5$	2.10	2.23394	4.0062
Day 2	$O_1, O_1, O_2, O_3, O_3, O_4, O_4, O_5$		2.24704	3.17175
Day 3	$O_2, O_1, O_2, O_3, O_3, O_2, O_2, O_5$		2.4923	3.23129
Day 4	$O_1, O_2, O_2, O_1, O_3, O_1, O_2, O_6$		2.47547	3.08055
Day 5	$O_1, O_3, O_2, O_1, O_3, O_5, O_2, O_4$		2.52337	3.1867
Day 6	$O_2, O_2, O_3, O_2, O_3, O_4, O_3, O_4$		2.72174	3.32432
Day 7	$O_1, O_2, O_1, O_3, O_3, O_5, O_3, O_6$		2.68091	3.28233

$$A^0 = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} = \begin{bmatrix} 0.53 & 0.26 & 0.16 & 0.05 \\ 0.36 & 0.50 & 0.08 & 0.06 \\ 0.11 & 0.21 & 0.52 & 0.16 \\ 0.03 & 0.07 & 0.18 & 0.72 \end{bmatrix} \tag{14}$$

$$B^0 = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} \\ b_{31} & b_{32} & b_{33} & b_{34} & b_{35} & b_{36} \\ b_{41} & b_{42} & b_{43} & b_{44} & b_{45} & b_{46} \end{bmatrix} = \begin{bmatrix} 0.72 & 0.11 & 0.08 & 0.04 & 0.03 & 0.02 \\ 0.60 & 0.14 & 0.11 & 0.10 & 0.03 & 0.02 \\ 0.03 & 0.01 & 0.06 & 0.3 & 0.2 & 0.4 \\ 0.07 & 0.05 & 0.09 & 0.3 & 0.13 & 0.36 \end{bmatrix} \tag{15}$$

$$\pi^0 = (0.7, 0.1, 0.1, 0.1) \tag{16}$$

Figure 9 shows that the risk value evaluated by experts is close to the other algorithms at the beginning of stage 1. It means that every assessment method is accurate at the beginning. After the beginning stage, the expert's assessment remains the same at each stage and cannot dynamically evaluate the system's security. HMM and DAF-ICSS assessment methods can dynamically assess the security of the system.

At the beginning of stage 2 in the assessment, we open the UDP port of the system, which leads to a new vulnerability. We increase the weight of V_v, and it results in a severe alarm state. However, the HMM assessment method draws an insensitive rise in Figure 9. Because the HMM method assigns no risk weight to a variety of system security states, DAF-ICSS can sensitively reflect the changes of system risk by weighing the evaluation elements and establishing a dynamic evaluation model. When the system is attacked by a UDP flood, the risk value assessed by DAF-ICSS exceeds CNY 40,000. The values given by other evaluation methods do not exceed CNY 40,000. DAF-ICSS assessment is more accurate than HMM.

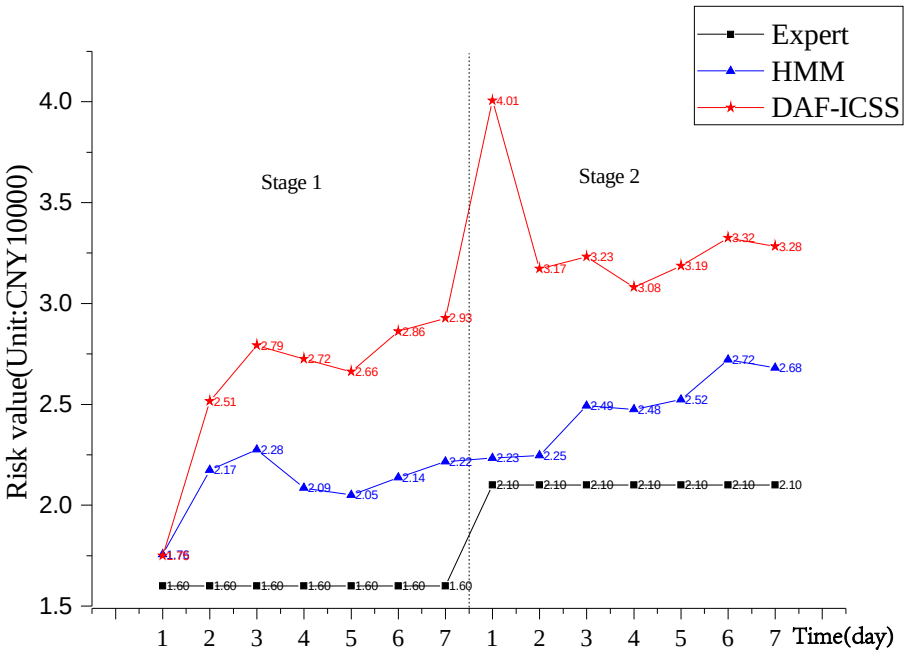

Figure 9. The result of the experiment.

Then, the evaluation system issues an alarm and closes the UDP port to lower the risk's value. The experiment confirms the effectiveness and timeliness of DAF-ICSS.

ICS may expose different vulnerabilities during running. For example, the operator opens the remote service port by mistake, which could lead to system vulnerability. We should focus on the dynamic changes in risk value. When the risk value suddenly increases, the system is probably experiencing a security risk.

The proposed framework of DAF-ICSS is more sensitive than other methods [42,43], which could provide a dynamical risk value. Table 11 lists the comparision of some security assessment methods in performance.

Table 11. The comparison of some security assessment methods in performance.

Method	Qualitative or Quantitative	Accuracy	Static or Dynamic	Evaluate Unknown Attacks
Expert	Qualitative	High accuracy	Static	Y
Fault tree	Qualitative	Medium accuracy	Static	N
Bayesian network	Quantitative	Medium accuracy	Static	N
HMM	Combination	Medium accuracy	Dynamic	Y
DAF-ICSS	Combination	High accuracy	Dynamic	Y

7. Disscusion

In addition to industrial robots, the proposed method can also be used for other industrial control systems. Some parameters in the method need to be evaluated based on a specific application scenario. For example, the work environment will be changed according to different scenarios. If we obtain a more accurate risk value, the sequence and state can be increased to enhance the quality of DAF-ICSS. It will also increase the computational burden of the system.

The security assessment combines the qualitative method, which uses a risk map to determine the system's security, and the quantitative method, which uses a risk value to measure security value. Because the assessment relies on observations of ICS anomaly

alarms, the risk value may be inaccurate when the alarms do not accurately match the system's state. In the future, it can be overcome to some extent.

8. Conclusions

Security assessment is the critical part of the system's security. We propose a security assessment method for ICS. We divide the security assessment of ICS into three steps: static recognition, dynamic monitoring, and assessment. A hierarchical system is provided for evaluating security risks. To obtain the system's risk level, the assessment method based on W-HMM calculates the industrial security risk value. It can be updated online for optimized estimation results and determine the degree of influence with different parameters in the factory. DAF-ICSS enables operators to find out a change of risk with high precision and efficiency. It also can be used to conduct cause analysis and security impact analysis.

However, this assessment method still has room for improvement, such as exploring methods for selecting more reasonable weights, etc. In addition, there is a well-known problem in industrial systems: The already designed secure architecture that does not sacrifice functionality has difficulty in providing a coordination of security and safety. In the future, we could focus on assessing multiple industrial control systems and fundamental understanding between safety and security based on dynamic security assessments so that dedicated modeling constructs and metrics can be proposed.

Author Contributions: Conceptualization, X.J.; Formal analysis, Y.C. and H.W.; Methodology, X.J. and G.W.; Data curation, H.W.; Software, H.W. and G.W.; Resources, H.W.; Funding acquisition & Project administration, Y.C.; Supervision, X.J.; Validation, Y.C.; Visualization, X.-F.J. and G.W.; Writing—original draft, X.J.; Writing—review & editing & Investigation, X.-F.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received the support of the National Key R&D Program of China (2019YFB1312202).

Data Availability Statement: Not applicable.

Acknowledgments: Projects supported by the National Key R&D Program of China (2019YFB1312202) are greatly acknowledged.

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A

The probability of the hidden state, S_i, at time, t, is expressed in Equation (A1). The probabilities of the hidden states that is S_i at time t and S_m at time $t+1$ are defined in Equation (A2). The Baum–Welch algorithm is used to calculate the model parameters for n times, as shown in Equations (A3)–(A5). The condition for terminating iteration is that the absolute values of $a_{ij}^{n+1} - a_{ij}^{n}$, $b_{ij}^{n+1} - b_{ij}^{n}$ or $\pi_i^{n+1} - \pi_i^{n}$ are within a tolerance criterion.

$$\gamma_t(i) = P(x_t = S_i \mid \lambda), \ \ 1 \le i \le 4 \tag{A1}$$

$$\xi_t(i,m) = P(x_t = S_i, \ x_{t+1} = S_m \mid \lambda), \quad 1 \leqslant i, m \le 4 \tag{A2}$$

$$a_{im}^{n+1} = \frac{\sum_{t=1}^{T-1} \xi_t(i,m)}{sum_{t=1}^{T-1} \gamma t(i)}, \quad (T \ is \ the \ length \ of \ Markov\ ) \tag{A3}$$

$$b_{ij}^{n+1} = \frac{\sum_{t=1,O_j}^{T-1} \gamma_t(i)}{\sum_{t=1}^{T} \gamma_t(i)} \tag{A4}$$

$$\pi_i^{n+1} = \gamma_1(i) \tag{A5}$$

References

1. Dieber, B.; Breiling, B.; Taurer, S; Rass, S.; Schartner, P. Security for the robot operating system. *Robot. Auton. Syst.* **2017**, *98*, 192–203. [CrossRef]
2. Tan, Q.; Tong, Y.; Wu, S.; Li, D. Towards a next-generation production system for industrial robots: A CPS-based hybrid architecture for smart assembly shop floors with closed-loop dynamic cyber physical interactions. *Front. Mech. Eng.* **2020**, *15*, 1–11. [CrossRef]
3. Cevallos, H.; Gualacio, J.; Silva, A.; Montalvo, P. Implementation of a Remote Control and Monitoring System in Assembly Processes with Industrial Robot Kawasaki Rs003 Through the GSM Network in the Industrial Automation Laboratory of the Faculty of Mechanics. *KnE Eng.* **2018**, *3*, 101–110. [CrossRef]
4. Li, L.; Xie, L.; Hao, B.; Yang, L.; Hu, T.; Wang, Z. Data Logic Attack on Heavy-Duty Industrial Manipulators. *IEEE Access* **2020**, *8*, 17419–17433. [CrossRef]
5. Bhardwaj, A.; Avasthi, V.; Goundar, S. Cyber security attacks on robotic platforms. *Netw. Secur.* **2019**, *2019*, 13–19. [CrossRef]
6. Robla-Gómez, S.; Becerra, V.M.; Llata, J.R.; Gonzalez-Sarabia, E.; Torre-Ferrero, C.; Perez-Oria, J. Working together: A review on safe human-robot collaboration in industrial environments. *IEEE Access* **2017**, *5*, 26754–26773. [CrossRef]
7. Wangen, G.; Hallstensen, C.; Snekkenes, E. A framework for estimating information security risk assessment method completeness. *Int. J. Inf. Secur.* **2018**, *17*, 681–699. [CrossRef]
8. Li, S.; Bi, F.; Chen, W.; Miao, X.; Liu, J.; Tang, C. An improved information security risk assessments method for cyber-physical-social computing and networking. *IEEE Access* **2018**, *6*, 10311–10319. [CrossRef]
9. Kumar, D.; Meeden, L. A robot laboratory for teaching artificial intelligence. *ACM SIGCSE Bull.* **1998**, *30*, 341–344. [CrossRef]
10. Das, S.; Mukhopadhyay, A.; Saha, D.; Sadhukhan, S. A markov-based model for information security risk assessment in healthcare MANETs. *Inf. Syst. Front.* **2019**, *21*, 959–977. [CrossRef]
11. Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E. Information security climate and the assessment of information security risk among healthcare employees. *Health Inform. J.* **2020**, *26*, 461–473. [CrossRef] [PubMed]
12. Turskis, Z.; Goranin, N.; Nurusheva, A.; Boranbayev, S. Information security risk assessment in critical infrastructure: A hybrid MCDM approach. *Informatica* **2019**, *30*, 187–211. [CrossRef]
13. Manickavasagam, K.; Prasad, B.K.S.; Ramasangu, H. Assessment of power system security using Security Information Index. *IET Gener. Transm. Distrib.* **2019**, *13*, 3040–3047. [CrossRef]
14. Yang, Y.; Zheng, X.; Sun, Z. Coal resource security assessment in China: A study using entropy-weight-based TOPSIS and BP neural network. *Sustainability* **2020**, *12*, 2294. [CrossRef]
15. Zhou, J.; Reniers, G.; Zhang, L. A weighted fuzzy Petri-net based approach for security risk assessment in the chemical industry. *Chem. Eng. Sci.* **2017**, *174*, 136–145. [CrossRef]
16. Smith, D.; Veitch, B.; Khan, F.; Taylor, R. Understanding industrial safety: Comparing Fault tree, Bayesian network, and FRAM approaches. *J. Loss Prev. Process. Ind.* **2017**, *45*, 88–101. [CrossRef]
17. Hu, L.; Li, H.; Wei, Z.; Dong, S.; Zhang, Z. Summary of research on IT network and industrial control network security assessment. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 1203–1210.
18. Alladi, T.; Chamola, V.; Zeadally, S. Industrial control systems: Cyberattack trends and countermeasures. *Comput. Commun.* **2020**, *155*, 1–8. [CrossRef]
19. Adil, M.; Khan, R.; Ali, J.; Roh, B.H.; Ta, Q.T.H.; Almaiah, M.A. An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. *IEEE Access* **2020**, *8*, 163209–163224. [CrossRef]
20. AlMedires, M.; AlMaiah, M. Cybersecurity in Industrial Control System (ICS). In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 640–647.
21. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Chen, S.; Liu, D.; Li, J. Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies* **2020**, *13*, 2509. [CrossRef]
22. Adil, M.; Khan, R.; Almaiah, M.A.; Binsawad, M.; Ali, J.; Al Saaidah, A.; Ta, Q.T.H. An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. *IEEE Access* **2020**, *8*, 148510–148527. [CrossRef]
23. Ratnayake, R.C. Consequence classification based spare parts evaluation and control in the petroleum industry. In Proceedings of the 2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Macao, China, 15–19 December 2019; pp. 1204–1210.
24. Adil, M.; Almaiah, M.A.; Omar Alsayed, A.; Almomani, O. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors* **2020**, *20*, 2311. [CrossRef] [PubMed]
25. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
26. Park, J.W.; Lee, S.J. A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence. *Ann. Nucl. Energy* **2020**, *142*, 107432. [CrossRef]

27. Xu, H.; Su, J.; Zong, X.; Yan, L. Attack identification for software-defined networking based on attack trees and extension innovation methods. In Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, Romania, 21–23 September 2017; pp. 485–489.
28. Shang, W.; Gong, T.; Chen, C.; Hou, J.; Zeng, P. Information security risk assessment method for ship control system based on fuzzy sets and attack trees. *Secur. Commun. Netw*. **2019**, *2019*, 3574675. [CrossRef]
29. Hu, J.; Guo, S.; Kuang, X.; Meng, F.; Hu, D.; Shi, Z. I-HMM-Based Multidimensional Network Security Risk Assessment. *J. Abbr.* **2019**, *8*, 1431–1442. [CrossRef]
30. Subramanian, N.; Zalewski, J. Quantitative assessment of safety and security of system architectures for cyberphysical systems using the NFR approach. *IEEE Syst. J*. **2014**, *10*, 397–409. [CrossRef]
31. Aziz, A.; Ahmed, S.; Khan, F.I. An ontology-based methodology for hazard identification and causation analysis. *Process. Saf. Environ. Prot*. **2019**, *123*, 87–98. [CrossRef]
32. Ye, Y.; Yan, L.; Sun, W.; Zhang, Q.; Wang, N. Discussion on Risk Assessment of Network Security Management. In Proceedings of the 2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Changsha, China, 10–11 February 2018; pp. 409–411.
33. Zou, Z.; Hou, Y.; Yang, H.; Li, M.; Wang, B.; Guo, Q. Research and implementation of intelligent substation information security risk assessment tool. In Proceedings of the 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 24–26 May 2019; pp. 1306–1310.
34. Chen, J.; Zhu, H.; Chen, Z.; Cai, X.; Yang, L. A Security Evaluation Model Based on Fuzzy Hierarchy Analysis for Industrial Cyber-Physical Control Systems. In Proceedings of the 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 11–12 November 2019; pp. 62–65.
35. Datta, S.K. DRAFT-A Cybersecurity Framework for IoT Platforms. In Proceedings of the 2020 Zooming Innovation in Consumer Technologies Conference (ZINC), Novi Sad, Serbia, 26–27 May 2020; pp. 77–81.
36. Park, K.C.; Shin, D.H. Security assessment framework for IoT service. *Telecommun. Syst.* **2017**, *64*, 193–209. [CrossRef]
37. He, D.; Deng, Z.; Zhang, Y.; Chan, S.; Cheng, Y.; Guizani, N. Smart contract vulnerability analysis and security audit. *IEEE Netw.* **2020**, *34*, 276–282. [CrossRef]
38. Holgado, P.; Villagrá, V.A.; Vazquez, L. Real-time multistep attack prediction based on hidden markov models. *IEEE Trans. Dependable Secur. Comput.* **2017**, *17*, 134–147. [CrossRef]
39. Tu, S. Derivation of Baum-Welch Algorithm for Hidden Markov Models. 2015. Available online: Https://people.eecs.berkeley.edu/~stephentu/writeups/hmm-baum-welch-derivation.pdf (accessed on 1 March 2022).
40. Tian, D.; Yang, B.; Chen, J.; Zhao, Y. A multi-experts and multi-criteria risk assessment model for safety risks in oil and gas industry integrating risk attitudes. *Knowl.-Based Syst.* **2018**, *156*, 62–73. [CrossRef]
41. Wang, C.; Li, K.; He, X. Network risk assessment based on baum welch algorithm and HMM. *Mob. Netw. Appl.* **2021**, *26*, 1630–1637. [CrossRef]
42. Aly, S.; Tyrychtr, J.; Kvasnicka, R.; Vrana, I. Novel methodology for developing a safety standard based on clustering of experts' assessments of safety requirements. *Saf. Sci.* **2021**, *140*, 105292. [CrossRef]
43. Budiyanto, M.A.; Fernanda H. Risk assessment of work accident in container terminals using the fault tree analysis method. *J. Mar. Sci. Eng.* **2020**, *8*, 466. [CrossRef]