Bayesian Network Based C2P Risk Assessment for Cyber-Physical Systems

XIAORONG LYU, YULONG DING, AND SHUANG-HUA YANG, (Senior Member, IEEE)

1Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
2Academy for Advanced Interdisciplinary Studies, Southern University of Science and Technology, Shenzhen 518055, China
3Department of Mathematics, Southern University of Science and Technology, Shenzhen 518055, China

Corresponding author: Shuang-Hua Yang (yangsh@sustech.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61873119 and Grant 61911530247.

ABSTRACT

Cyber-Physical Systems (CPS) refer to a new generation of intelligent systems with integrated computational performance and physical capabilities. However, with the expansion of system complexity and the enhancement of system openness, most CPS become not only safety-critical but also security-critical since they involve physical objects, computer networks and communications. In the past decade, it is no longer rare to see safety incidents and security attacks happening in industries. Identifying risks in CPS is critical to ensure the normal operation of these systems. The Cyber-to-Physical (C2P) risk is defined as the impact of cyber threats on physical process safety. In this paper, a C2P risk assessment model based on hierarchical Bayesian Network (BN) is proposed, and the feasibility of this model is verified by constructing two undesired event scenarios on a typical CPS. The quantitative risk values are explained and compared through qualitative risk analysis and assessment.

INDEX TERMS

Cyber-physical systems, CPS, C2P risk, risk assessment, Bayesian network.

I. INTRODUCTION

A. CYBER-PHYSICAL SYSTEMS

Cyber-Physical Systems refer to a new generation of intelligent systems with integrated computational performance and physical capabilities [1]. Sensing the state of the physical system by data acquisition devices, analyzing the data through computation and controlling the physical entities by sending instructions, construct the basic closed loop of automatic data flow and form a fusion between the physical part and the cyber part.

Among the physical and cyber parts, physical objects, people, the environment, sensors, actuators, and devices that interact with the outside world play a different role in the physical world. Computing, control, and network communication technologies act as information shells to digitize physical entities and provide interactive interfaces to the physical world and the information world, enabling remote control of physical entities. The information shell is a bridge for physical information exchange between physical devices. Through the information shell, the physical device is connected with the information world, and the physical space and information space are integrated [2], [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.
monitor risk control and financial resources to mitigate the adverse effects of loss. There are two kinds of risk management approaches. One is reactive approaches focusing on incident/disaster response, and the other is proactive approaches focusing on prevention and preparation. Risk assessment often consists of three steps – risk identification, risk analysis and risk evaluation. The risk assessment process is a “key component” of the risk management process. Generally, there are two categories of risk analysis and assessment methods, i.e., qualitative and quantitative methods. The qualitative assessment methods largely rely on expert experience and focus on revealing the nature of the risks, while the quantitative assessment methods can calculate the risk value of the system and focus on the quantitative performance of the system under the risks. In general, the quantitative methods are preferred to conduct risk analysis and assessment, because their accurate descriptions of system risks can facilitate the optimization of the allocation of protection resources.

C. SAFETY AND CYBER-SECURITY RISK ASSESSMENT FOR CPS

There is a lot of work carried out in risk assessment for CPS in recent years. Safety risk assessment has been well developed for CPS. For example, Liu et al. [5] proposed a risk assessment approach for the cascading failure of electric CPS caused by the failure of the control function of the information system. The method of combining Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA) and Bayesian Network was adopted to infer the safety risk of the Large Phased Array Radar (LPAR) software system [6]. Among the most popular ones are FTA, FMEA and Hazard and Operability Study (HAZOP) [7].

Security risk assessment has become a hot topic in CPS recently. Attack Trees Analysis (ATA) and System Theoretic Process Analysis (STPA) are widely used for security risk assessment. Nourian and Madnick [8] utilized a system theoretic framework to evaluate and enhance the security of CPS. Sheela et al. [9] presented a systematic approach to estimate cyber risks for intelligent and non-intelligent attacks in power system. Zhu et al. [10] presented a hierarchical flow model (HFM) for accessing the impact of cyber attacks on critical infrastructures.

Safety and security issues are increasingly converging on CPS, leading to new situations in which these two closely related issues should be considered together, rather than separately or in sequence. Kornecki et al. [11] studied the relationship between the functional safety and cyber-security of CPS through Bayesian Network to determine the impact of low-level equipment failures on the functional safety and cyber-security of the entire CPS, and evaluated the risk at these two domains respectively. Subramanian and Zalewski apply [12] adapted the NFR approach to quantitatively evaluate the safety and security properties of CPS to mitigate and control the risks of CPS. Sabaliauskaitė and Adepu [13] proposed the Six-Step Model (SSM) and Information Flow Diagram (IFD) integration approach to enable comprehensive CPS safety and security analysis.

The existing approaches of risk assessment for CPS from the perspectives of safety, security and their integration were reviewed in [14]. This work compared some available approaches and identified the current situation of safety and security issues in CPS. Although there have been many experts and scholars that studied the problem of CPS risk analysis and assessment from the perspectives of functional safety, cyber-security as well as integrated security risk analysis, they mostly consider the functional safety and cyber-security of the systems independently. However, the safety and security between the cyber domain and the physical domain will affect each other.

D. CONTRIBUTIONS

In the literature, most studies only analyse and evaluate the cyber domain security risks of CPS. Security in CPS includes not only cyber-security, but also functional safety. Most current probabilistic risk assessment schemes based on Bayesian Network pay more attention to cyber-security at the cyber level but ignore the impact of cyber threat on physical process safety, which we define as Cyber-to-Physical (C2P) risk. Most attacks at the cyber level will lead to serious functional safety accidents. This study intends to analyse and evaluate the C2P risks of both cyber domain and physical domain of Cyber-Physical Systems by building a Bayesian Network.

In this paper, a C2P Risk Assessment model is proposed and verified. The main contributions of this paper are outlined as follows:

1) We define the C2P risk to quantify the impact of cyber threat on physical process safety in CPS.
2) We design a new C2P risk assessment model based on hierarchical Bayesian Network. It is a probabilistic approach for studying how undesired events propagate from the cyber domain to the physical domain and their impacts.
3) We propose a new method to calculate the C2P risk based on the proposed C2P risk assessment model.

To demonstrate the feasibility of our approach, a CPS example is simulated, and two undesired event scenarios are constructed. Our risk assessment model is constructed and compared with qualitative risk assessment. Case study shows that the results of the two methods are consistent with each other.

The rest of this paper is organized as follows. Section II discusses the related work, and explains the rationality of using BN. Our risk assessment model and the new method of calculating the C2P risk are illustrated in Section III. Case study is presented in Section IV to demonstrate our model. Finally, we discuss the proposed new model and method in general in Section V and conclude our work in Section VI.
II. BAYESIAN NETWORK IN RISK ASSESSMENT

A. RISK ASSESSMENT THEORY

In Cyber-Physical Systems, risk refers to both the functional safety risk and cyber-security risk, which is the adverse impact caused by the destruction of the system security objectives. The overall objective of the risk assessment process is to identify risks and their impact on the system assets. Even though the impact on CPS could be various, tangible or intangible, such as life loss, economical loss, deterioration of environment, or damage to reputation, in this study we limit the impact of Cyber-to-Physical risk on CPS to system asset loss. While compound security risks will be identified later in the system life cycle, the goal of this phase is to identify the security risks of assets based on threat/vulnerability pairings. Therefore, Vulnerability, Threat and Asset are the three factors that determine the risk level of system security. Vulnerabilities are a part of system components that can be exploited, leading to the loss of an asset. Threats are potential sources of damage to system assets. Capitals are tangible or intangible assets that are valuable to an enterprise and need to be protected. The basic risk calculation model can be summarized as (1).

\[ R = f(h(V, T), A) \]  

where \( R \) is the risk value, \( f \) is the risk model, \( h \) represents the relationship between threats and asset loopholes. \( V \) and \( T \) represent the possibility of exploitation of the vulnerability and the probability of threats to exploit vulnerabilities respectively. \( A \) is the asset value.

B. BAYESIAN NETWORK

Bayesian Network (BN) is used to describe the probability graph model between different random variables. It is an effective tool for the analysis and inference of uncertain events.

Definition 1 ([15]): If \( G \) is a Directed Acyclic Graph (DAG), \( \Theta \) indicates a Conditional Probability Distribution (CPDs), then formula for the Bayesian Network is defined as \( B = (G, \Theta) \), where
- graph (qualitative) component: directed acyclic graph (DAG) \( G = (V, E) \), where \( V \) is a set of vertices (nodes) representing \( n \) discrete random variables \( X = \{X_1, X_2, \ldots, X_n\} \), \( E \) is a set of directed edges (arcs) corresponding to the conditional dependency between these variables.
- numerical (quantitative) component: a set of parameters \( \Theta = \{\Theta_1, \Theta_2, \ldots, \Theta_n\} \), \( \Theta_i \) = \( P(X_i|\text{Parent}(X_i)) \) is defined as the conditional probability distribution of the node \( X_i \) given its the parent node \( \text{Parent}(X_i) \) state, which is usually stored and grouped in a tabular form named Conditional Probability Table (CPT).

A Bayesian Network contains two types of nodes, i.e. parent node and child node. The node at the beginning of any directed edge is called the parent node (cause), and the node at the end is called the child node (fruit). The directed edge indicates that the two nodes are correlated. In particular, a node without a parent is called a root node, and a node without children is called a leaf node.

As it can be seen from the definition, the Bayesian Network can be used to simulate a causal relationship (also called conditional dependencies). Event Probability, depicting the connection between attributes or objects, is a representation of a Joint Probability Distribution (JPD). Given a set of random variable \( X = \{X_1, X_2, \ldots, X_n\} \), the JPD can be expressed as (2).

\[ P(X) = P(X_1, X_2, \ldots, X_n) = P(X_1)P(X_2|X_1) \cdots P(X_n|X_1, X_2, \ldots, X_n-1) = \prod_{i=1}^{n} P(X_i|\text{Parent}(X_i)) \]  

C. BAYESIAN NETWORK IN RISK ASSESSMENT

BN is an increasingly popular modelling technique in cyber-security fields such as forensic, risk management and smart grid security [16]–[19]. Currently, there are some probabilistic risk assessment methods based on Bayesian Network for CPS, but most of them are converted from IT systems. Similar to the work presented in [20], [21], where Bayesian Network was used to evaluate the security risk of the cyber domain of the power system, and analyse the reliability of the power system. To evaluate the CPS system security risks, Qi et al. [22] proposed a multi-model Bayesian Network, which describes risk propagation through attack models, functional models and accident models. Zhang and Zhang [23] analyzed the CPS cyber-security risk by establishing Bayesian model based on Petri Nets. Zhang et al. [24] proposed a dynamic probabilistic risk assessment model based on fuzzy Bayesian Network, which to some extent, solved the problem of the lack of historical data by using a fuzzy approximation dynamic recommendation algorithm. This model can evaluate the cyber-security risk of CPS in practice. Meyur [25] proposed a Bayesian attack tree based approach to model cyber attack and to assess the associated cyber-physical security risk of power systems.

We define the Cyber-to-Physical risk as the impact of cyber threat on physical process safety in CPS. To the best of our knowledge, little work has been done in C2P risk assessment. We believe BN suits the need of C2P risk assessment due to the following reasons. Firstly, CPS has a hierarchical structure and BN simulates a causal relationship which can easily describe the layers in the CPS hierarchy. Secondly, the propagation of the impact of cyber-attacks within the CPS hierarchy is acyclic. BN is by default an acyclic graph with conditional dependencies between connected nodes. Thirdly, BN can help to identify, understand and quantify complex interrelationships between nodes. If C2P risk factors are described by the BN nodes they can emerge and be connected to each other to represent the propagation process of the C2P risk in CPS. Finally, historical data are often lacking in conducting risk assessment for CPS. The previous study by Greitzer et al. [26] indicated BN outperforms other
III. RISK ASSESSMENT MODEL

A. CYBER-PHYSICAL SYSTEM HIERARCHY

A typical Cyber-Physical System can be divided into four layers: the physical process layer, the field control layer, the process monitoring layer, and the enterprise management layer as shown in Fig. 1. Various device connections and inter-communication constitute the Cyber-Physical System. The main control, Human Machine Interface (HMI), and database are located in the process monitoring layer. The main control unit is responsible for sending control instructions down to the field control layer and transmitting sensor data up to the main control unit. Remote terminal units (RTU), sensors, and actuators are located in the field control layer and interact with the physical process layer.

B. C2P RISK ASSESSMENT MODEL BASED ON BAYESIAN NETWORK

1) ASSET ANALYSIS

Determining the assets to be protected is a key step in risk analysis and assessment, and a necessary prerequisite for inferring the overall risk of the system. The depth and rigor of the asset analysis process should be commensurate with the depth and rigor of the overall security risk assessment of the system. Asset analysis can be as simple as listing the items to be protected based on available inventory and engineering judgement, or as complex as equipment inventory, traceability matrix of system resources, and review of legal documents. CPS assets analysis includes the following steps:

Step 1: Collect and analyse the design documents, description documents of the CPS, or conduct research and interviews with the relevant personnel of the system.

Step 2: Classify the assets of the system. The assets are generally divided into tangible assets and intangible assets. System assets can be divided into data assets, software assets, physical assets, people and intangible assets according to the Cyber-Physical System hierarchy. Data assets contain data stored in real time and historical databases, as well as system configuration files, etc. Software assets refer to the applications of the system; physical assets include communication equipment, industrial control equipment, data acquisition equipment and other control equipment; personnel includes system operators and managers; intangible assets refer to the public image and reputation of the enterprise related to the system.

Step 3: Summarize and generate a list of assets of the CPS in the form of Table 1, and determine the valuation of each asset.

2) BUILDING BAYESIAN NETWORK

a: STRUCTURING BAYESIAN NETWORK

The vulnerability of Cyber-Physical Systems needs to be determined by various vulnerability scanning tools, with the consideration of the probability of hazards using frequency approximation of the vulnerability obtained by system experts and/or from historical data that has been exploited by the attacker. The system vulnerability information can be obtained from the Common Vulnerabilities and Exposures (CVE) database according to the configuration of each layer of the system, so as to obtain the hierarchical Bayesian Network topology structure. Assuming that there is an undesired security event scenario, the C2P risk of the system under a given condition can be calculated through the Bayesian Network. According to the hierarchical structure of Cyber-Physical Systems, the typical structure of Bayesian Network for analysing C2P risk is shown in Fig. 2 where $A_i$ represents the asset in the management layer, $S_j$ represents the asset in the monitoring layer, $C_i$ denotes asset in the field control layer including all kinds of controllers and other assets, $P_i$ denotes physical assets, $V_{A_i}$ represents the vulnerability of each asset in the management layer, $V_{S_j}$ represents the vulnerability assets of the process in the monitoring layer, $V_{C_i}$ represents the vulnerability of the assets in the field control layer, $\bigcirc$ represents the component assets in the various layers of the Cyber-Physical System and $\Box$ represents the vulnerabilities in which each component asset itself may be exploited.
There are two ways to establish the CPT in practical applications: assign the CPT values according to the background knowledge of the domain experts; calculate the CPT values from the corresponding frequencies in the data set. The first approach is subjective, and finding experts in the field is difficult. If node variables are not observed in the dataset, the process of finding CPT parameter values in the second approach becomes complicated. In fact, the number of elements in CPT could be very large due to the complex interdependencies among the nodes in the BN. Any change in the relationship among the nodes can affect the entire network, thus making the determination of conditional probability table an intractable problem in Bayesian Network modelling.

In order to measure the conditional probability distribution of each node, it is necessary to first estimate the probability that a security incident successfully compromises the target system by exploiting certain vulnerabilities. The calculation of this probability is related to each directed edge in the Bayesian Network as well as the probability of the parent node reaching the child node. NIST’S second version of the Common Vulnerability Scoring System (CVSS) defines that, the vulnerability is successfully exploited according to the combination of Access Vector (AV), Access Complexity (AC) and Authentication (AU). Zangeneh and Shajari [27] proposed to estimate the probability of the vulnerability being successfully exploited by $P_{\text{exploitability}} = C \cdot AV \cdot AC \cdot PR \cdot UI$.

CVSS basic metrics quantify the difficulty in resource vulnerability utilization. Table 2 summarizes the basic metrics of CVSS and the scores, which can be obtained from the CVSS v3.0 user guide [29].

The successful exploitation of a certain vulnerability in CVSS of NIST is normalized, as shown in (3).

$P_{\text{exploitability}} = \frac{C}{F} \cdot AV \cdot AC \cdot PR \cdot UI$ (3)

where $P_{\text{exploitability}}$ is the probability of the vulnerability being successfully exploited. $C$ denotes exploitation factor. $F$ denotes the upper limit of the exploitation score. $AV$, $AC$, $PR$ and $UI$ represent the metric of the access vector, the metric of the attack vector, the metric of the required permissions for intervention and the metric of the user interaction respectively.

| Factor | Factor Scale | Value |
|--------|--------------|-------|
| Access vector | Network access (N) | 0.85 |
| | Near network access (N) | 0.62 |
| | Local (L) | 0.55 |
| | Physical medium (P) | 0.20 |
| Access complexity | Low (L) | 0.77 |
| | High (H) | 0.44 |
| Permits needed for access | No authentication (N) | 0.85 |
| | Single user authentication (L) | 0.62 |
| | Multi-user authentication (H) | 0.27 |
| User interaction | No user operation needed to get access (N) | 0.85 |
| | User operations needed to get access (R) | 0.62 |

The successful exploitation of a certain vulnerability in CVSS of NIST is normalized, as shown in (3).
probability can be calculated by (5).

\[
P(X_i | \text{Parent}(X_i)) = \begin{cases} 
0, & \text{if } \forall x_j \in \text{Parent}(X_i), \ x_j^i = 0 \\
\prod_{x_j^i = 1} (1 - P(e_i)), & \text{otherwise} 
\end{cases} 
\]

(5)

In (4) and (5), \(P(X_i | \text{Parent}(X_i))\) represents conditional probability of node \(X_i\). \(X_i\) and \(X_j\) represent nodes in Bayesian Network. Parent(\(X_i\)) is the parent node of node \(X_i\), \(e_i\) denotes the event of successfully exploiting the vulnerability of node \(X_i\) and passes the risk from the parent node \(X_j\) to \(X_i\). \(X_j^i\) denotes the state of node \(X_j\), being successfully compromised or not. \(1X_j^i = 1\) means success, \(X_j^i = 0\) means failure.

The introduction of the two logic gates can help us get the bayesian conditional probability distribution of each node in the network and enable the quantitative risk assessment in the form of probability. Bayesian Network can visually show the connection between the security incidents and calculate the occurrence of system failures caused by security events. Taking the risk model shown in (1), replacing the risk model \(f\) with SUM operator, the relationship between threat and asset vulnerabilities \(h\) with the Bayesian Network, the C2P risk of a CPS could be derived as follows.

\[
\text{Risk} = \sum_{i=1}^{m} V_{A_i} \times P(A_i | \text{Parent}(A_i)) 
\]

(6)

where \(A = \{A_i\}\) represents system assets, \(i = \{1, 2, \ldots, m\}\). \(V_{A_i}\) is the value of the assets. \(P(A_i | \text{Parent}(A_i))\) denotes the probability of asset loss.

IV. CASE STUDY

In this section, the feasibility of the proposed C2P risk assessment model for Cyber-Physical Systems based on Bayesian Network is demonstrated by constructing two undesired event scenarios for a double-tank process.

A. AN EXAMPLE OF CYBER-PHYSICAL SYSTEMS

The quadruple-tank process proposed by Johansson is simplified as a double-tank process [31], which is a typical Cyber-Physical System including a cyber part and a physical part. The system structure is shown in Fig. 3.

The physical part is simulated on an individual simulation host (SH), including a dual tank, control elements, Level sensor and execution elements (pump and regulator). In addition to the physical process simulation, the hardware-in-the-loop test platform includes the following components.

1. There are administrator host (AH) and several user machines (PC1, . . ., PCN) and the Database Server (DBS1) at the top layer.
2. The system master control centre (HMI) and database server (DBS2) designed and implemented in the monitoring network layer.
3. Programmable Logic Controller (PLC) is a common Controller. In the field control layer, there are two controllers (PLC1, PLC2).
4. The physical process layer includes a manual control valve, an electric control valve, an upper water pump and two liquid level sensors.

Among them, the enterprise communication network is directly connected to the Internet, the process monitoring layer is isolated from the enterprise network through a firewall F1, and only the administrator host has the right to manage the monitoring network. Another firewall F2 is deployed in the field control layer, through which the system master control centre and the database server can transfer data to the PLC controllers. Other devices in the monitoring layer communicate with each other through the Modbus transmission control protocol of the industrial ethernet. The Gateway (GW) between the monitoring and control layers is responsible for protocol transformation. The controller is connected to the CAN bus of the control network and communicates with the simulation host (SH). The part in the light grey box in Fig. 3 is realised on the simulation host.

B. ASSET LIST

According to the method described in Section III-B.1, a list of assets of the double-tank CPS can be obtained, as shown in Table 3.

Lack or weakness of security protection in CPS could be catastrophic depending on the application. For example, security violations in smart grids could lead to the loss of services to the consumer and financial losses to the utility company. If the security of CPS in a nuclear plant has been compromised, the possible consequence could be loss of life and permanent damage to the environment in the region. As we mainly consider industrial CPS (iCPS) and the inherent
security vulnerabilities in the legacy control systems and their communications in this study, the impact of C2P risk is quantified as the loss of assets in iCPS. Furthermore, for the sake of simplicity without losing the generality, the costs of purchasing the assets are used as the asset values, as shown in Table 4.

### C. BAYESIAN NETWORK CONSTRUCTION

It is assumed that the liquid level control system has the inherent vulnerability as shown in Table 5, and the vulnerability information was taken from the public vulnerability information database CVE and the National Vulnerability Database (NVD).

According to the vulnerability information of each asset of the system described in Table 5, a Bayesian Network is constructed, as shown in Fig. 4. Among them, AH represents the administrator host, HMI represents the man-machine interaction interface of the monitoring centre, DBS represents the database in the system, $C_1, C_2$ represent two controllers at the field control layer, $V$ represents the valve, $P$ represents the pump, and Tank represents the water tank. In Fig. 4, the logical relationship between the nodes is as follows: $v_0 \text{“or” } v_1 \text{“or” } v_2 \text{“or” } v_3 \text{“or” } v_4 \text{“or” } v_5 \text{“or” } v_6 \text{“or” } v_7 \text{“or” } HMI \text{“and” } DBS \text{“and” } (v_8 \text{“or” } v_9)$. The probability of successful exploitation of each asset vulnerability node in the system can be calculated by (3), where $\text{AV}, \text{AC}, \text{PR}$ and $\text{UI}$ can be found from NVD. The individual values of $\text{AV}, \text{AC}, \text{PR}$ and $\text{UI}$ are given by using the CVSS basic metric shown in Table 6 [30].

![Bayesian Network topology of double-tank CPS.](image)

### D. C2P RISK ANALYSIS

1) UNDESIRED EVENT SCENARIO CONSTRUCTION

The objective of calculating the C2P risk value in an undesired event scenario is to provide guidance and advice for

![Bayesian Network topology of double-tank CPS.](image)
TABLE 8. Conditional probability distribution of node AH.

| AH       | AH<sup>0</sup> | AH<sup>1</sup> |
|----------|----------------|----------------|
| P(AH = AH<sup>0</sup> | 1 | 0 |
| P(AH = AH<sup>1</sup> | 0.273 | 0.272 |
| P(AH = AH<sup>0</sup> | 0.075348 | 0.924652 |
| P(AH = AH<sup>1</sup> | 0.866 | 0.134 |
| P(AH = AH<sup>0</sup> | 0.236418 | 0.763582 |
| P(AH = AH<sup>1</sup> | 0.236418 | 0.763582 |
| P(AH = AH<sup>0</sup> | 0.064542114 | 0.935457886 |

TABLE 9. Conditional probability distribution of node DBS.

| DBS     | DBS<sup>0</sup> | DBS<sup>1</sup> |
|---------|----------------|----------------|
| P(DBS = DBS<sup>0</sup> | 1 | 0 |
| P(DBS = DBS<sup>1</sup> | 0.273 | 0.272 |
| P(DBS = DBS<sup>0</sup> | 0.075348 | 0.924652 |
| P(DBS = DBS<sup>1</sup> | 0.866 | 0.134 |
| P(DBS = DBS<sup>0</sup> | 0.236418 | 0.763582 |
| P(DBS = DBS<sup>1</sup> | 0.236418 | 0.763582 |
| P(DBS = DBS<sup>0</sup> | 0.064542114 | 0.935457886 |

TABLE 10. Conditional probability distribution of node HMI.

| HMI     | HMI<sup>0</sup> | HMI<sup>1</sup> |
|---------|----------------|----------------|
| P(HMI = HMI<sup>0</sup> | 1 | 0 |
| P(HMI = HMI<sup>1</sup> | 0.273 | 0.272 |
| P(HMI = HMI<sup>0</sup> | 0.075348 | 0.924652 |
| P(HMI = HMI<sup>1</sup> | 0.866 | 0.134 |
| P(HMI = HMI<sup>0</sup> | 0.236418 | 0.763582 |
| P(HMI = HMI<sup>1</sup> | 0.236418 | 0.763582 |
| P(HMI = HMI<sup>0</sup> | 0.064542114 | 0.935457886 |

TABLE 11. Conditional probability distribution of node C<sub>i</sub>(i = 1, 2).

| C<sub>i</sub> | C<sub>i</sub><sup>0</sup> | C<sub>i</sub><sup>1</sup> |
|-------------|----------------|----------------|
| P(C<sub>i</sub> = C<sub>i</sub><sup>0</sup> | 1 | 0 |
| P(C<sub>i</sub> = C<sub>i</sub><sup>1</sup> | 0.273 | 0.272 |
| P(C<sub>i</sub> = C<sub>i</sub><sup>0</sup> | 0.075348 | 0.924652 |
| P(C<sub>i</sub> = C<sub>i</sub><sup>1</sup> | 0.866 | 0.134 |
| P(C<sub>i</sub> = C<sub>i</sub><sup>0</sup> | 0.236418 | 0.763582 |
| P(C<sub>i</sub> = C<sub>i</sub><sup>1</sup> | 0.236418 | 0.763582 |
| P(C<sub>i</sub> = C<sub>i</sub><sup>0</sup> | 0.064542114 | 0.935457886 |

TABLE 12. Conditional probability distribution of node P.

| P       | P<sup>0</sup> | P<sup>1</sup> |
|---------|--------------|--------------|
| P(P = P<sup>1</sup> | 0.956 | 0.044 |

TABLE 13. Conditional probability distribution of node V.

| V       | V<sup>0</sup> | V<sup>1</sup> |
|---------|--------------|--------------|
| P(V = V<sup>1</sup> | 1 | 0 |
| P(V = V<sup>0</sup> | 0.9375 | 0.0625 |

TABLE 14. Conditional probability distribution of node Tank.

| Tank    | Tank<sup>0</sup> | Tank<sup>1</sup> |
|---------|----------------|----------------|
| P(Tank = Tank<sup>0</sup> | 1 | 0 |
| P(Tank = Tank<sup>1</sup> | 0.922 | 0.078 |
| P(Tank = Tank<sup>0</sup> | 0.875 | 0.125 |
| P(Tank = Tank<sup>1</sup> | 0.80675 | 0.19325 |

the safe and reliable operation of Cyber-Physical Systems. To illustrate the proposed C2P risk assessment method, we constructed the following two undesired event scenarios:

1. Scenario 1: By exploiting the Windows Search remote code execution vulnerability v<sub>1</sub>, attackers could obtain the local access permission of the administrator’s host AH as well as the remote access permission to HMI of the water level control system.

2. After obtaining the system control authority, the intruder illegally uses the system management identity to enter the main control centre, uses the industrial ethernet Modbus protocol vulnerability to initiate a man-in-the-middle-attack and send a fake packet within the normal range to the upper-level database server, uses the database vulnerability v<sub>4</sub> to write the fake data into the database, and modify the controlled liquid level value of the lower tank through the vulnerability v<sub>5</sub>

3. By exploiting v<sub>8</sub>, the lower layer controller sends malicious code to invalidate the controllers C<sub>1</sub>, C<sub>2</sub>, causing the original system to fail to maintain the normal liquid level as the upper layer of the database server still receives the fake data within the normal range, where the administrator cannot locate the attack in time. In severe cases, the water pressure in the sealed...
water tank may be too high causing the water tank to burs, endangering the environment and workers.

In this scenario, the operation state of the real liquid level control system is disordered. The change of liquid level in the upper and lower water tanks is shown in Fig. 5. The opening degree of the pump is shown in Fig. 6. In Fig. 5, the yellow curve represents the desired value of the water level of the lower tank maintaining at 0.5, the red curve represents the change of the water level of the lower tank after the attack, and the blue represents the change of the water level of the upper tank. Fig. 6 illustrates the failure of the automatic control function of the pump. Obviously, the expected state of the liquid level control system has been destroyed, and the liquid level of the lower tank cannot be maintained at the desired value 0.5.

(2) Scenario 2: The liquid level sensor is responsible for data collection, and the illegal intruder uses the Modbus protocol to trigger the attack and enable the forged data transmission vulnerabilities $v_3$. Noise is maliciously added to the data during transmission on the industrial ethernet. Assuming this noise is written into the database which makes the water level value lower than the real value. The controller will mistakenly assume that, the opening of the pump is not enough, thus adjusting the degree of the water pump. This will cause the liquid level of the lower tank to increase instantaneously, causing the water in the lower tank to overflow.

2) C2P RISK ANALYSIS AND ASSESSMENT

We constructed the Bayesian Network through the visual modelling environment of GeNIe as shown in Fig. 7. The probability of loss of each asset in the double-tank CPS is calculated under each undesired event scenario, based on the Bayesian Network model.

For Scenario 1: The evidence chain is $v_4^1 = v_4^1, v_4^2 = v_4^1, v_5^3 = v_5^5, v_6^8 = v_8^8$, the probability of asset AH loss is $P(AH | v_4^1, v_2^2, v_5^5) = 0.73169042$, the probability of asset DBS loss is $P(DBS^1 | v_3^3, v_4^4, AH^1) = 0.084551614$, and the probability of asset HMI loss is $P(HMI^1 | v_5^5, v_6^6, v_7^7, AH^1) = 0.23672395$, the probability of loss of controller $C_1$ is $P(C_1^1 | v_3^3, v_4^4, DBS^1) = 0.0065530546$, the probability of loss of controller $C_2$ is $P(C_2^2 | v_5^5, v_6^6, DBS^1) = 0.0065530546$, the probability of loss of pump P is $P(P | C_3^1) = 0.99373528$, the probability of loss of valve V is $P(V | C_2^2) = 0.062090434$ and the probability that the asset Tank will lose is $P(Tank | P^1, V^1) = 0.12845744$. According to (6), it can be obtained that the C2P Risk value of the system in this scenario is $Risk_1 \approx 0.986418$.

Similarly, for Scenario 2: The evidence chain is $v_3^4 = v_3^4$, under which the probability of asset AH loss is $P(AH | v_1^1, v_2^2, v_5^5) = 0.031471221$, the probability of asset DBS loss is $P(DBS^1 | v_3^3, v_4^4, AH^1) = 0.020380717$ and the probability of asset HMI loss is $P(HMI^1 | v_5^5, v_6^6, v_7^7, AH^1) = 0.00061601483$, the probability of loss of controller $C_1$ is $P(C_1^1 | v_3^3, v_4^4, DBS^1) = 6.6027434 \times 10^{-6}$, the probability of loss of controller $C_2$ is $P(C_2^2 | v_5^5, v_6^6, DBS^1) = 6.6027434 \times 10^{-6}$, the probability of loss of pump P is $P(P | C_3^1) = 0.99999369$, the probability of loss of valve V is $P(V | C_2^2) = 0.062499587$ and the probability that the asset Tank will lose is $P(Tank | P^1, V^1) = 0.12926481$. According to (6), it can be obtained that the C2P Risk value of the system in this security event scenario is $Risk_2 \approx 0.247611$.

In the above two scenarios, since the evidence chain in the first scenario is more sufficient than that of the second scenario, for the former, all assets of the system have been successfully exploited, while for the latter, only the vulnerability of DBS has been successfully exploited. Intuitively, each asset of the system is more likely to be affected in the first scenario than in the second scenario and the risk of the system is correspondingly higher. The result of quantitative analysis is $Risk_1 \approx 0.986418 > Risk_2 \approx 0.247611$, which also proves that the system under the first scenario has a higher C2P Risk value.
### TABLE 15. PI Matrix in NIST.

| Risk level | Impact degree |
|------------|---------------|
|            | L(10) M (50) H(100) |
| H(1.0)     | L(10) M(50) H(100) |
| M(0.5)     | L(5) M(25) M (50) |
| L(0.1)     | L(1) L(5) L (10) |

### TABLE 16. Five-grade division of probability scale.

| Probability scale | VH | H | M | L | VL |
|-------------------|----|---|---|---|----|
| Probability range  | (80, 100) | (50, 80) | (20, 50) | (1, 20) | [0, 1] |

### TABLE 18. Five-level risk assessment matrix.

| Risk level | Impact degree |
|------------|---------------|
| VH(5)      | M(50) H(50) M(150) VH(50) |
| H(4)       | L(40) N (50) H(120) H(160) VH(200) |
| M(3)       | L(30) M(60) M(90) H(120) H(150) |
| L(2)       | L(20) L(40) M(60) M(90) H(100) |
| VL(1)      | VL(10) VL(20) L(30) L(40) M(50) |

### TABLE 19. The degree of probability and importance of the loss caused by the threat source attack on the assets of the system components.

| Scenario1 | Probability rank | Importance degree |
|-----------|------------------|--------------------|
| AH        | H                | M                 |
| DBS       | L                | M                 |
| HMI       | VL               | VH                |
| C1, C2    | L                | VL                |
| P         | VL               | VL                |
| V         | L                | L                 |
| Tank      | L                | L                 |

### FIGURE 8. Risk level of each asset in Scenario 1.

In Section I, we mentioned that qualitative assessment and quantitative assessment are two basic methods of risk assessment. Qualitative assessment methods show the consequences of incidents by directly providing numerical estimation, which is the concrete description of risks. Qualitative risk assessment is the subjective judgement and abstract representation of risks by analysing the probability and influence of security events to determine the priority of risks (that is, to rank the severity of risks). Qualitative assessment of the severity of risks can avoid cumbersome, complex and controversial valuation process and is simple and easy to operate. Compared with the qualitative assessment methods, the qualitative assessment methods can obtain the results quickly but not provide a numerical value.

Instead of assigning numerical (or monetary) values to components and losses, qualitative assessments rank the influence of each element. For example, NIST sp800-30 classifies risk as “high”, “medium”, and “low” [32]. The Probability and Impact Matrix (PI Matrix) are used to determine the risk level. The Probability and Impact of each component are classified into three levels: high, medium and low. The combination of probability and impact can be used to determine the risk level. The probability and impact scales can be in numbers (1, 5, 10, etc.), text (high, medium, low), or color coding (red, yellow, green). Table 15 shows the NIST probability / impact risk rating matrix, where H, M, and L indicate High, Medium, and Low.

We refine the five levels based on the NIST’s risk classification to produce the probability scale and impact degree (or the importance degree of the asset) as shown in Tables 16 and 17. On this basis, the refined matrix of risk assessment is obtained, as shown in Table 18, where, VH, H, M, L and VL respectively represent the probability scale, impact degree and risk level as “very high”, “high”, “medium”, “low” and “very low”. Obviously, the closer the cell is to the upper right, the higher the risk level (severity it gets).

According to Tables 16 and 17, the probability level of loss caused by threat source attack and the importance degree of each component under the two scenarios are obtained respectively through experts, as shown in Table 19. In these scenarios, AH, DBS, HMI, C1, C2, P, V and Tank respectively represent component assets of previously studied double-tank CPS.

Bubble chart can visually present the risk level of each asset component of the system under different scenarios, as shown in Fig. 8 and Fig. 9. The size and color of the bubble reflect the severity of the risk, and the bigger and darker the bubble is, the greater the risk it represents.

Intuitively, the risk levels of each asset in Fig. 8 are generally higher than those in Fig. 9 at the top right. Therefore, at the system level, the risk is higher in Scenario 1 than in Scenario 2.

In summary, the results in qualitative risk assessment and quantitative risk assessment are consistent with each other. The risk value obtained from quantitative evaluation is endowed with practical significance. The value of risk
The risk assessment method for iCPS proposed in this study contributes to the field by providing a definition of the Cyber-to-Physical risk and developing a BN based method of quantifying the C2P risk. This new C2P risk assessment model inherits the hierarchical BN topology and well describes the layers in the iCPS hierarchy. Furthermore, the propagation process of the C2P risk in iCPS is conducted through the BN nodes representing the assets of iCPS or C2P risk factors. The safety risk caused by cyber-security is seamlessly embedded in the risk propagation process. The limitations of the C2P risk assessment method proposed in this study are twofold. Firstly, the new assessment method is based on a static BN model, and does not suit for dynamic risk assessment. Secondly, the impact of C2P risk is limited to asset loss quantified by the asset purchasing cost in this study. The impact of C2P risk could be in a wide range, both tangible and intangible, and the asset value loss is only a typical tangible impact.

Compared with the existing risk assessment approaches, this study focuses on the impact of cyber threat on physical process safety. The risk at the system level is quantified as the asset value loss. Even though it is not convincing to directly compare the new C2P risk assessment method with the existing approaches due to different focuses, the qualitative risk analysis method at the asset level is applied to the two same scenarios as the one assessed by the C2P risk assessment method. The assessment results obtained from both methods support each other.

VI. CONCLUSION
This paper proposed a C2P risk analysis model for Cyber-Physical Systems based on Bayesian Network. Through CVE, the possible vulnerability of each asset component is found, and the structure of Bayesian Network is constructed. The probability of successful exploitation of vulnerability attacker is obtained according to CVSS vulnerability scores. The conditional probability distributions (CPDs) of non-root node in Bayesian Network is obtained by logic gates (“and” and “or”). C2P risk analysis model can be used to obtain the C2P risk value of CPS. Through the construction of two specific undesired scenarios for a double-tank water system and comparing with qualitative risk assessment, the feasibility of the proposed C2P risk analysis and assessment model are verified.

The proposed BN based method provides an integrated solution to the C2P risk assessment for industrial CPS. The foundation of the method is the Bayesian Network which is a static model. By extending the Bayesian Network into a dynamic Bayesian Network, the work could be enhanced for the dynamic C2P risk assessment. In addition, the impact of C2P risk is limited at asset purchasing cost in this study. Considering the impact of C2P risk could be various, such as life loss, economical loss, deterioration of environment, or damage to reputation, the future work could be done in quantifying a wide range of the impacts of C2P risk including tangible and/or intangible assets.
REFERENCES

[1] Y. Qi, “Energy scheduling based remote estimation in cyber-physical systems,” Ph.D. dissertation, Dept. Control Eng., Zhejiang Univ., Zhejiang, China, 1993.

[2] N. Guo and C. Jia, “White paper on cyber physical systems 2017,” (in Chinese), Inf. Technol. Standardization, no. 4, pp. 37–41, 2017.

[3] N. Guo and C. Jia, “White paper on cyber physical systems 2017,” (in Chinese), Inf. Technol. Standardization, no. 5, pp. 43–48, 2017.

[4] N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and J. M. R. Tavares, “Medical cyber-physical systems: A survey,” J. Med. Sci., vol. 42, no. 4, 2018, Art. no. 74.

[5] Y. Liu, D. Lu, L. Deng, T. Bai, K. Hou, and Y. Zeng, “Risk assessment for the cascading failure of electric cyber-physical system considering multiple information factors,” IET Cyber-Phys. Syst., Theory Appl., vol. 2, no. 4, pp. 155–160, Dec. 2017.

[6] L. Xia, J. Yang, H. Wang, and X. Hou, “Safety analysis and risk assessment of LPAR software system,” in Proc. 12th ICRMS, Shanghai, China, 2018, pp. 150–154.

[7] J. V. Dunjó and J. A. L. I. F. Iñenakis Ichez Arnaldos, “Hazard and operability (HAZOP) analysis. A literature review,” J. Hazardous Mater., vol. 173, nos. 1–3, pp. 19–32, Jan. 2010.

[8] A. Nourian and S. Madnick, “A systems theoretic approach to the security threats in cyber physical systems applied to evaluation of a gas system,” IEEE Trans. Depend. Sec. Comput., vol. 15, no. 5, pp. 1–13, Oct./Nov. 2018.

[9] A. Shela, S. Revathi, and A. Iqbal, “Cyber risks assessment for intelligent and non-intelligent attacks in power system,” in Proc. 2nd ICEDPC, Chennai, India, Aug. 2019, pp. 40–45.

[10] Q. Zhu, Y. Qin, C. Zhou, and L. Fei, “Hierarchical flow model-based impact assessment of cyberattacks for critical infrastructures,” IEEE Syst. J., vol. 13, no. 4, pp. 3944–3955, Dec. 2019.

[11] A. J. Kornecki, N. Subramanian, and J. Zalewski, “Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on Bayesian belief networks,” in Proc. FedCSIS Kraków, Poland, Sep. 2013, pp. 1393–1399.

[12] N. Subramanian and J. Zalewski, “Quantitative assessment of safety and security of system architectures for cyberphysical systems using the NFR approach,” IEEE Syst. J., vol. 10, no. 2, pp. 397–409, Jun. 2016.

[13] G. Sabaliauskaite and S. Adepou, “Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security,” in Proc. 10th Int. Symp. HASE, Singapore, Jan. 2017, pp. 41–48.

[14] X. Lyu, Y. Ding, and S.-H. Yang, “Safety and security risk assessment in cyber-physical systems,” IET Cyber-Phys. Syst., Theory Appl., vol. 4, no. 3, pp. 221–232, 2019.

[15] P. Leray and O. Francois, “Common cyber security vulnerabilities observed in control system assessments by the INL NSTB program,” INL, Idaho Falls, ID, USA, Tech. Rep. INL/EXT-08-13979, 2008.

[16] N. Poolsapatt, R. Dewri, and I. Ray, “Dynamic security risk management using Bayesian attack graphs,” IEEE Trans. Depend. Sec. Comput., vol. 9, no. 1, pp. 61–74, Jan. 2012.

[17] S. Chockalingam, W. Pieters, A. Teixeira, and P. van Gelder, “Bayesian network models in cyber security: A systematic review,” in Proc. NordSec, Tartu, Estonia, 2017, pp. 105–122.

[18] Y. Wadhawan, A. AlMajali, and C. Neuman, “A comprehensive analysis of smart grid systems against cyber-physical attacks,” Electronics, vol. 7, no. 10, p. 249, 2018.

[19] L. Mu noz-González, D. Sgandurra, M. Barrière, and E. C. Lupu, “Exact inference techniques for the analysis of Bayesian attack graphs,” IEEE Trans. Depend. Sec. Comput., vol. 16, no. 2, pp. 231–244, Mar./Apr. 2019.

[20] Y. Zhang, Y. Xiang, and L. Wang, “Reliability analysis of power grids with cyber vulnerability in SCADA system,” in Proc. IEEE PES Gen. Meeting Conf. Expo., Harbor, MD, USA, Jul. 2014, pp. 1–5.

[21] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, “Power system reliability evaluation with SCADA cybersecurity considerations,” IEEE Trans. Smart Grid, vol. 6, no. 4, pp. 1707–1721, Jul. 2015.

[22] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, “Multimodel-based incident prediction and risk assessment in cybersecurity protection for industrial control systems,” IEEE Trans. Syst., Man, Cybern. Syst., vol. 46, no. 10, pp. 1429–1444, Oct. 2016.

[23] X. Zhang and D. Zhang, “Quantitative risk assessment of cyber physical power system using Bayesian based on Petri net,” in Proc. 5th IEEE Int. Conf. CCDS, Nanjing, China, Nov. 2018, pp. 988–992.

[24] Q. Zhang, C. Zhou, Y.-C. Tian, N. Xiong, Y. Qin, and B. Hu, “A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems,” IEEE Trans. Ind. Informat., vol. 14, no. 6, pp. 2497–2506, Jun. 2018.

[25] R. Meyur, “A Bayesian attack tree based approach to assess cyber-physical security of power system,” in Proc. IEEE TPEC, College Station, TX, USA, Feb. 2020, pp. 1–6.

[26] F. L. Greitre, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer, “Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats,” in Proc. 45th Hawaii Int. Conf. Syst. Sci., Maui, HI, USA, Jan. 2012, pp. 2392–2401.

[27] V. Zangeneh and M. Shajari, “A cost-sensitive move selection strategy for moving target defense,” Comput. Secur., vol. 75, pp. 72–91, Jun. 2018.

[28] FIRST. (2015). Common Vulnerability Scoring System Version 3.0: Specification Document Version 3.0. [Online]. Available: https://www.first.org/cvss/specification-document

[29] FIRST. (2015). Common Vulnerability Scoring System Version 3.0: User Guide, Version3.0. [Online]. Available: https://www.first.org/cvss/v3.0/user-guide

[30] FIRST. (2015). Common Vulnerability Scoring System Version 3.0: Calculator Use & Designe, Version3.0. [Online]. Available: https://www.first.org/cvss/v3.0/use-design

[31] K. H. Johansson, “The quadruple-tank process: A multivariable laboratory process with an adjustable zero,” IEEE Trans. Control Syst. Technol., vol. 8, no. 3, pp. 456–465, May 2000.

[32] A. Rot, “Computer support of risk analysis in information technology environment,” in Proc. SAM, Las Vegas, NV, USA, 2009, pp. 283–284.

XIAORONG LYU received the B.S. degree in E-commerce from Northwest A&F University, Shaanxi, China, in 2017, and the M.S. degree in computer science and technology from the Southern University of Science and Technology, Shenzhen, China, in 2019. Her research interest includes safety and security of cyber-physical systems.

YULONG DING received the B.A.Sc. and M.A.Sc. degrees in chemical engineering from Tsinghua University, China, in 2005 and 2008, respectively, and the Ph.D. degree in chemical engineering from The University of British Columbia, Canada, in 2012. He is currently a Research Assistant Professor with the Academy for Advanced Interdisciplinary Studies, Southern University of Science and Technology. His main interests are industrial Internet of Things and low-power wide area networks (LPWANs).

SHUANG-HUA YANG (Senior Member, IEEE) received the B.S. degree in instrument and automation and the M.S. degree in process control from the China University of Petroleum (Huadong), Beijing, China, in 1983 and 1986, respectively, and the Ph.D. degree in intelligent systems from Zhejiang University, Hangzhou, China, in 1991. He is currently the Chair Professor of computer science with the Southern University of Science and Technology, China. His current research interests include cyber-physical systems, the Internet of Things, wireless network-based monitoring and control, and safety critical systems. He is a fellow of IET and InstMC, U.K. He is also an Associate Editor of IET Cyber-Physical Systems: Theory and Applications, the International Journal of Computing and Automation, and the Journal of InstMC.

VOLUME 8, 2020