International Journal of Information Security
https://doi.org/10.1007/s10207-022-00608-4

SPECIAL ISSUE PAPER

Dependency-based security risk assessment for cyber-physical systems

Aida Akbarzadeh[1] · **Sokratis K. Katsikas**[1]

Abstract
A cyber-physical attack is a security breach in cyber space that impacts on the physical environment. The number and diversity of such attacks against Cyber-Physical Systems (CPSs) are increasing at impressive rates. In times of Industry 4.0 and Cyber-Physical Systems, providing security against cyber-physical attacks is a serious challenge which calls for cybersecurity risk assessment methods capable of investigating the tight interactions and interdependencies between the cyber and the physical components in such systems. However, existing risk assessment methods do not consider this specific characteristic of CPSs. In this paper, we propose a dependency-based, domain-agnostic cybersecurity risk assessment method that leverages a model of the CPS under study that captures dependencies among the system components. The proposed method identifies possible attack paths against critical components of a CPS by taking an attacker's viewpoint and prioritizes these paths according to their risk to materialize, thus allowing the defenders to define efficient security controls. We illustrate the workings of the proposed method by applying it to a case study of a CPS in the energy domain, and we highlight the advantages that the proposed method offers when used to assess cybersecurity risks in CPSs.

Keywords Cyber-physical systems · Attack path analysis · Risk assessment · Safety · Security · Industrial control systems · Industry 4.0

1 Introduction

The merging of Information and Communication Technology (ICT) with Operational Technology (OT) has formed Cyber Physical Systems. The advantages of this merging in the monitoring and control of traditional industrial control systems notwithstanding [1], the interdependencies between the cyber and the physical parts of CPSs cause new types of cybersecurity risks, as cyber components may adversely affect the physical environment, thereby increasing safety risks. For instance, in the Maroochy attack, by leveraging the cyber parts of the Maroochy county water service, an attacker gained remote access to the control system which enabled him to affect pumping stations [2]. He gradually discharged 800,000 L of raw sewage into the river; this had a severe impact on nature reserves, on wildlife, as well as on the local population. Stuxnet [3] and attack to Florida water treatment plant [4] are two other examples of cyber-physical attacks.

In a CPS, unexpected events mainly stem from the overly convoluted connections and interdependencies among its heterogeneous components. Castellanos et al. [5] shed light on the new risks that direct and undirect dependencies between cyber and physical components bring to Industrial Control Systems (ICSs) that form the core of cyber-physical systems. These dependencies further accentuate when the CPS is a system-of-systems. Alcaraz et al. [6] also reviewed the emerging challenges of protecting industrial control systems and pointed out the fact that the different mindsets between IT and OT operators regarding the security risk in CPSs is one of the main reasons that these dependencies are still neglected.

The diversity of assets and of the interactions among them in a CPS is an additional reason why traditional risk assessment methods are not able to identify cyber physical attacks, as the scope of analysis in these methods is limited to pure IT systems. Recent works have proposed merging previously developed security and safety risk assessment methods. However, these integrated methods do not address the cyber-physical and physical-cyber interdependencies in

✉ Aida Akbarzadeh
aida.akbarzadeh@ntnu.no

Sokratis K. Katsikas
sokratis.katsikas@ntnu.no

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

Published online: 22 August 2022

the assessment, as the constituents have been developed separately, with focus on either the physical or the cyber facets of CPSs. Indeed, traditional CPSs were built as physically and logically isolated systems, air-gaped systems, with no security mechanisms in place except for physical security measures. Later, these systems were gradually augmented with networking functionality and could connect to the Internet and provide remote monitoring and control [7].

Cyber-physical systems are known as complex systems, and this characteristic mainly stems from the multiple types of connections, different system topologies and various structures of subsystems in a cyber-physical system. Moving toward Industry 4.0 will significantly increase this complexity. Consequently, systems comprising identical assets may face different security risks. As a result, risk assessment should focus on the interactions and relations between the assets of a CPS rather than merely on the assets themselves. This requires a precise investigation from the physical field devices up to the cyber management systems to cover every aspect of the system; in other words, an "end-to-end" investigation is required to cover both IT and OT with a unified approach.

The IEC TS 62351-1:2007 standard [8] states that providing 100% security for each system component not only counts as a costly and impractical solution, but also might discourage enterprises attempting to utilize security mechanisms. Therefore, risk assessment methods for CPSs need to pay special attention to increasing the efficiency and avoiding unnecessary analysis that is of no value to enhancing the security of the system. Wang et al. [9] also stated that attacks to CPSs have unique characteristics, as adversaries have a clear attack target and aim to damage the operational part of the systems to different extent. As a result, improving the security of CPSs highly depends on extracting the sequence of attack steps toward the adversaries' target. This implies that risk assessment methods in CPSs should follow a goal-oriented approach, to enhance effectiveness and improve accuracy.

One approach to conduct an end-to-end risk assessment is to leverage attack path analysis [10]. An attack path specifies an attack scenario and a sequence of assets that can be used by attackers to reach to their goal. Indeed, each attack composed of different phases that must be proceed step-by-step to reach its final objective, known as "kill chain" [11]. In other words, each attack could be seen as a chain of dependency. Therefore, to prevent the attacker from reaching its goal and influence the system, it is enough to break the linkages of this chain. Only one disruption in the attack path can protect the system. Accordingly, a new notion for an "end-to-end" protection can be defined, in which the "end-to-end" safety and security implies the absence of a dependency chain between the two corresponding components. In this case, security and safety flaws of individual assets are accepted as long as adversaries cannot leverage them to make a semantic path within the system. However, attack path analysis is an IT-related method whose main focus is to understand how attackers gain access to their victim asset and which vulnerabilities can be exploited on which assets. Cyber-physical systems are different in nature; this should be considered when developing a method based on attack path analysis. Besides, the emerging cyber-physical attacks have shown that in many cases adversaries attempt to interrupt the physical process of the system or to damage physical components that are supposed to be isolated by air gaps [12–14]. Unlike IT systems, affecting the functionality of industrial control systems is most often the target of complex cyber attacks in CPSs. Therefore, a unified IT&OT risk assessment, i.e., a general risk assessment of a CPS, requires the contribution of OT experts to clear the goal of potential attacks toward field devices on one hand, and of IT experts to provide a complete picture of how an attacker might be able to reach their target component and affect the system on the other.

Acknowledging the advantages of leveraging attack path analysis to draw a clear picture of possible attacks against a CPS and considering the specific attributes of CPSs, in this paper we propose a novel, dependency-based risk assessment method. The method first identifies the critical assets of the system and then, discovers chains of dependencies between pertinent assets that might be leveraged by attackers to reach their target. The proposed method is a comprehensive method that considers both the topological and functional relationships between the system components as direct and hidden dependencies within the CPS, to provide a holistic risk assessment. It utilizes Bow Tie modeling for visualizing security risks to facilitate the collaboration between IT and OT experts in CPSs and assists the defenders in understanding the intention of attackers, thus guiding them to employ relevant approaches to mitigate the accordant risks. It also helps defenders to discover those potential attack paths that may be created in case of a zero-day vulnerability. The proposed method is domain-agnostic and has been developed to cover all CPSs in different domains, such as Maritime, Aviation and Energy. In this work, we showcase the workings of the proposed method in a case study of a CPS in the energy domain, as an example.

The main contribution of this paper is as follows: We propose a dependency-based risk assessment method to extract goal-oriented attack paths in CPSs that considers cyber-physical and physical-cyber interdependencies within the systems. The proposed method:

- Facilitates the collaboration between IT and OT experts to identify unwanted events from both safety and security perspectives based on the Bow Tie model.

- Reveals complex cyber-physical attacks by employing backtrack analysis to understand the intention of attackers.
- Improves the effectiveness of attack path analysis by replacing blind analysis with goal-oriented backtrack analysis.
- Is a realistic method to compute risk and to assess Likelihood and Impact based on metrics that cover both IT and OT requirements.

The remainder of the paper is organized as follows: Sect. 2 reviews the related work. We describe the proposed method in Sect. 3, and a case study to expound the application of the proposed method is presented in Sect. 4. We discuss our findings in Sects. 5 and 6 summarizes our conclusions and indicates directions for future work.

2 Related work

A wealth of security risk assessment methods applicable to general purpose IT systems exists [15]. Even though several of these methods can be and have been applied to Cyber Physical Systems, they cannot accurately assess cyber risks related to CPSs [16]. Among different methods, threat modeling approaches such as STRIDE [17], Factor Analysis of Information Risk (FAIR) [18] and OCTAVE [19] have been applied to assess risk in CPSs operating in various domains. Combining two or more methods, mainly STRIDE and CVSS, is also a common approach to achieve better performance [20].

Alcaraz et al. [6] reviewed the emerging challenges of protecting industrial control systems and pointed to the urgent necessity of developing new mechanisms and recommendations. The authors argued that the integration of old technologies such as SCADA systems with modern communication networks and the different mindsets of IT and OT operators regarding the security risk is the core underlying factor that escalates these challenges and affects the security of the systems. In a follow-up paper, the authors studied different aspects of control systems in CPSs and concluded that OT assets such as RTUs and Data historians are of the most targeted and vulnerable assets in a CPS due to the fact that targeting these components not only imposes risks to sensitive information but also to the operational activities and processes in the system and all the dependent subsystems.

Cyber risk assessment methods for CPSs more often than not are domain specific, as they need to take into account safety as an impact factor additional to the "traditional" impact factors of confidentiality, integrity, and availability. This is why security and safety of CPSs are studied jointly. A comprehensive survey of security and safety co-engineering methods is provided in [21]. An overview of risk assessment methods specific to the smart grid case is provided in [22]. Kandasamy et al. [23] presented an overview of risk assessment methods for the Internet of Things. A review of risk assessment methods for SCADA systems is presented in [24]. Threat and risk assessment techniques for the automotive domain are reviewed in [25].

A number of approaches for risk assessment for CPSs, published before 2015, are listed in [16]. The list is not exhaustive, nor do the authors indicate how the listed works were selected. A more recent review of a few risk assessment methods for CPS, from the perspective of safety, security, and their integration, including a proposal for some classification criteria was made in [26].

Recently, Stellios et al. [7] proposed a high-level risk assessment approach for IoT-enabled cyber-physical systems with the emphasis on the identification of attack paths and explained the necessity for considering connectivity attack paths and functionality attack paths in CPSs. However, their work is limited to guidance, without any technical detail or case study.

Existing risk assessment methods for CPSs consider only the cyber or the physical part of the system, while cyber-physical and physical-cyber interdependencies are by and large left unattended. For example, Homer et al. [27] only considered the cyber parts of the system, while the authors in [28] focused on the physical parts. This is despite that, as Krotofil et al. [29] showed, attackers can leverage the physics of the process underlying a CPS to conduct their attack. The same authors suggested that when defining security measures, the physical process layer should be considered as well. As mentioned in [30], a holistic approach to studying the cyber physical systems is required which can handle the complex coupling between the physical process and the IT infrastructure.

However, to the best of our knowledge, a risk assessment method that satisfies this requirement has not been proposed. The method proposed in this paper addresses this research gap. Indeed, unlike existing methods, the method proposed herein facilitates the analysis of the entire cyber-physical system, for each unwanted event. Thus, it provides a clear picture of involved parts of the system and reveals the hidden dependencies and the potential infiltration points across the system.

3 Risk assessment methodology

This section describes the structure of the proposed risk assessment methodology. As shown in Fig. 1, the proposed method is divided into four phases. To conduct a holistic risk assessment for cyber-physical systems, we first need to model the system, to find connections and dependencies between the system components; this is done in Phase I. This will facilitate the identification of dependency chains and

the use of the bow-tie methodology which will be described later, in Phase III. Once we have modeled the system, we identify and rank the criticality of the system components, as the proposed method begins the risk analysis with the vital components; this is done in Phase II. Considering the numerous components that constitute a CPS, in particular a large-scale cyber-physical system, this approach enhances efficiency and enables system owners with limited information and resources to apply the proposed risk assessment method only to critical components in their system; however, a complete analysis is always recommended. In Phase III, for each target component selected according to the result of Phase II, we perform a depth-first search to extract dependency chains. Then, we identify all unwanted events for the target components and investigate whether each extracted dependency chain can actually lead to that unwanted event. It is worth mentioning that the main goal of this phase is to enable both IT and OT operators to investigate the preconditions that can lead to a specified unwanted event, from both a safety and a security perspective. Additionally, as the unwanted events can affect both the safety and the security of a system, it is required to consider the risk from both perspectives. Risk is generally computed based on the Likelihood of an event occurring and the resulting Impact of the event. Therefore, to calculate risk, we collect pertinent metrics to measure Likelihood and Impact form both a safety and a security perspective. This will be described in further detail in Phase III. Finally, after computing the risk of each identified dependency chain, we rank the results. In the following, we describe each phase in more detail.

3.1 Phase I: Model the system

Presenting a comprehensive model of a CPS appropriate for assessing cybersecurity risks requires capturing both the topological and functional aspects of the system. Therefore, the first step is to capture the connections within the system and identify the cyber and physical interactions in the system which denote the data flows and the material flows in the system, respectively. A method that has been widely applied in recent works to model a CPS is graph theory [31,32]. Using graph theory, a CPS is modeled as a directed graph $G(V, E)$ in which V is a set of vertices (nodes) representing the components of the system and E is a set of edges (links) representing interconnections between the system components.

3.2 Phase II: Identify and rank the critical components in the system

The goal of this step is to rank the criticality of the system components as potential targets for cyber physical attacks, from both the system and the organizational perspective. This

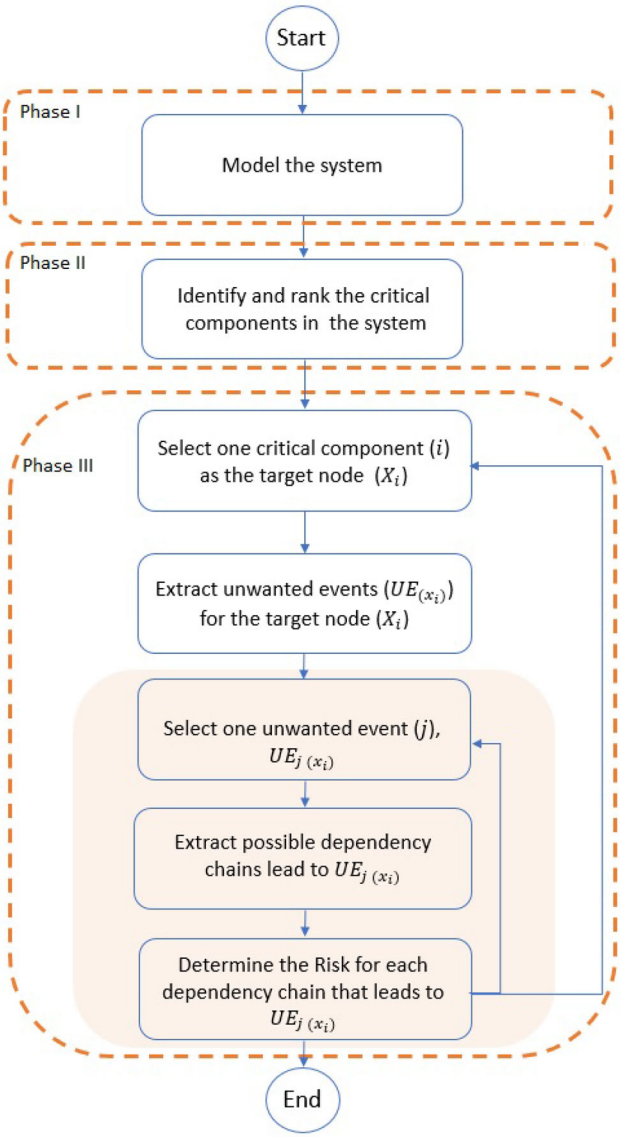

Fig. 1 Proposed risk assessment method

provides a macroscopic view of the system components and measures how important each component is, in case of accidental failures or deliberate attacks.

At the system level, the method presented in [33] is applied to measure the criticality. According to this method, the contribution of the system components, both the links and nodes, in preserving the system functionality and connectivity is evaluated. In more detail, the method of [33] utilizes the Closeness Centrality (CC) and two other novel graph metrics, namely the Tacit Input Centrality (TIC) and the Tacit Output Centrality (TOC), to measure the importance of nodes and links in a CPS. Then, by means of a multiple attribute decision making (MADM) approach, it aggregates these three metrics into the so-called Z-index and ranks the components of the CPS according to their criticality.

At the organizational level, the assistance of the system owners is required, as various factors such as economic effect and environmental effect are involved in the determination of the criticality. Indeed, at the system level, the main focus is solely on the characteristics and roles of the components, while at the organizational level, different aspects should be considered, e.g., the cost of repair and maintenance of the system components. Stakeholders assign one of the following values to determine the importance of each component at the organizational level:

- 1: Low importance;
- 2: Medium importance;
- 3: High importance.

Since the organizational level criticality is measured qualitatively, it should be scaled properly before aggregating with the result of the system level criticality. The overall criticality of a component X_i is calculated based on Eq. 1, in which C_{Org} and C_{Sys} refer to the organizational level criticality and the system level criticality, respectively.

$$C_{\text{Total}}(X_i) = \frac{C_{\text{Org}}(X_i)}{\max(C_{\text{Org}})} \times \max(C_{\text{Sys}}) + C_{\text{Sys}}(X_i) \qquad (1)$$

3.3 Phase III: Dependency-based risk assessment

3.3.1 Extract dependency chains

Adversaries tend to target critical components in a system. Therefore, this step aims to identify possible chains of dependencies between the system components that might be leveraged by attackers to reach their desire goal. In an ideal situation, the risk assessment proposed in this paper begins with the most vital components ranked in phase II and continues to the level of criticality that the system owners are satisfied with. Clearly, it is possible to apply the method to all components. As illustrated in Fig. 1, phase III begins with selecting one of the critical components of the system as the target node X_i. Next, all unwanted events $\text{UE}_{(X_i)}$ that might affect node X_i are identified. It should be noted that the term *unwanted event* means *top event* in safety risk assessment and *incident* in cybersecurity risk assessment [34].

Then, one of the unwanted events that can influence node X_i is selected for further study (i.e., $\text{UE}_{j(X_i)}$). By performing a depth-first search, all the non-circular dependency chains that terminate at X_i are discovered.

In order to conduct the cybersecurity risk analysis along with the dependency chain, we apply the concept of bow-tie methodology. Since bow-tie modeling provides a visual representation of the hazards/threats and corresponding unwanted events, it can facilitate risk analysis in CPSs and bridge the gap between experts with different backgrounds

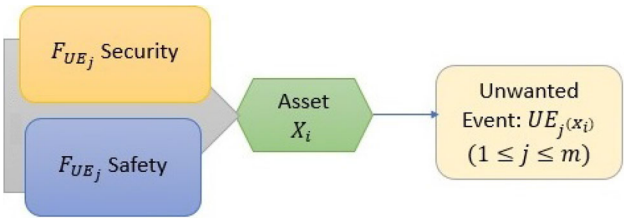

Fig. 2 Bow-tie

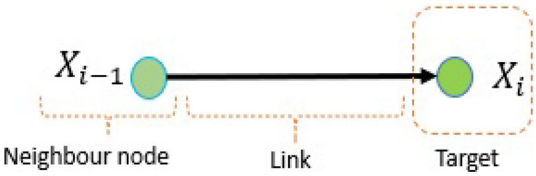

Fig. 3 Investigation of relationships in a dependency chain

and knowledge (e.g., IT and OT). The bow-tie analysis has been broadly used in safety risk management to identify root causes and consequences of hazards. Bernsmed et al. [34] applied bow-tie modeling to study the cybersecurity risks of maritime navigational systems and provided a common terminology for both safety and security risks which is adapted in our method. As depicted in Fig. 2, the right side of the bow-tie in our work corresponds to unwanted events ($\text{UE}_{j(x_i)}$) that might occur, the left side specifies the causes (F_{UE_j}) that can lead to these unwanted events, and the central knot marks the asset under study (X_i).

Assume that for the critical node X_i, $\text{UE}_{(X_i)} = \{\text{UE}_{1(X_i)}, \ldots, \text{UE}_{m(X_i)}\}$ are m possible unwanted events. To discover the attack paths that target node X_i, we start from node X_i and select the first unwanted event ($\text{UE}_{1(X_i)}$). Then, we check potential hazards and threats that can lead up to that event by considering node X_i, node X_{i-1} and link (X_{i-1}, X_i) as the corresponding attack surface of X_i (see Fig. 3).

If the cause of $\text{UE}_{1(X_i)}$ is found (called F_{UE_1}), we move one step to the left of the chain and repeat the same process for the next node (i.e., X_{i-1}). F_{UE_1} is any vulnerability or failure mode that can cause $\text{UE}_{1(X_i)}$. This process will terminate when there is no cause and effect relation between the neighbor nodes in a chain; the last node under the study denotes the *infiltration point* into the system (Fig. 4).

Considering asset X_i, F_{UE_j} points to the pre-condition j which, if met, will allow the post-condition (i.e., the unwanted event) $\text{UE}_{j_{(x_i)}}$ to occur. From the safety perspective, the pre-condition determines the failure modes and considers damage to property including X_i, X_{i-1} and link (X_{i-1}, X_i), while the post-condition shows the final effects and consequences of materializing each pre-condition. From the security perspective, affecting the confidentiality, integrity and availability is part of the pre-

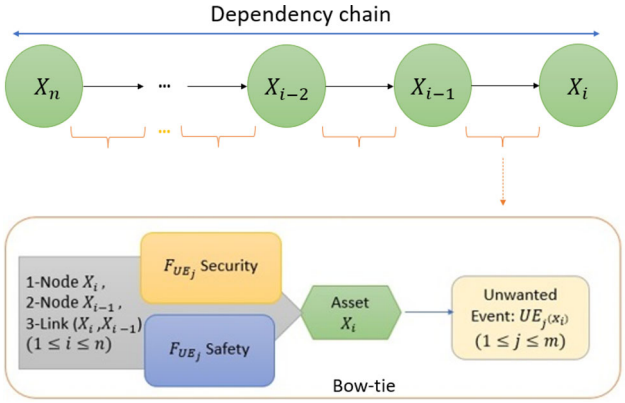

Fig. 4 Dependency chain and joint safety security risk analysis

condition, and the post-condition represents the goal of an attacker when targeting X_i, X_{i-1} or link (X_{i-1}, X_i).

It is worth emphasizing that, unlike previous works, we applied a backtracking approach to increase efficiency. Due to the fact that the goal of the risk assessment is clear from the beginning, here the attack paths and afterward the risk to each target component X_i can be computed separately with no need to investigate all the interactions and dependencies within a system. This approach also enables operators to view the system from the attackers' perspective and detect new attack paths that might exploit vulnerabilities that have been neglected during the system design.

To make it clear, consider the simple graph of Fig. 5. In this example, suppose that we are interested to detect attack paths that terminate at X_1 and cause $\mathrm{UE}_{1_{(x_1)}}$. Here, we assume that vulnerabilities and failure modes exist between $X_7 \rightarrow X_3 \rightarrow X_1$ and $X_{12} \rightarrow X_9 \rightarrow X_5 \rightarrow X_1$ that can be leveraged by attackers and consequently lead to $\mathrm{UE}_{1_{(x_1)}}$. Following the proposed method, we start the investigation from X_1 and move backwards to neighbor nodes $\{X_3, X_4, X_5\}$. Referring to the assumption, since there is no pre-condition F_{UE_j} that can lead to $\mathrm{UE}_{1_{(x_1)}}$ from X_5, investigation from node X_5 will be terminated and this node will be removed from the list. The investigation continues until Path 1 and Path 2 are found. Notice that in Path 2, although there is a link between X_{12} and X_{13}, the process of detecting attack path terminates at X_{12} for the same reason explained earlier. Now, imagine that one attempts to discover the same attack paths by performing the straightforward approach. In this case, s/he should discover all paths terminating at X_1 and starting at the rest of nodes (i.e., $\{X_2, X_3, \ldots, X14\}$) to make sure that all the attack paths have been extracted. Therefore, not all identified attack paths will be related to the target component X_1 and the unwanted event $UE_{1_{(x_1)}}$, as follows:

$$X_{14} \rightarrow X_{13} \rightarrow X_{10} \rightarrow X_6 \rightarrow X_2$$

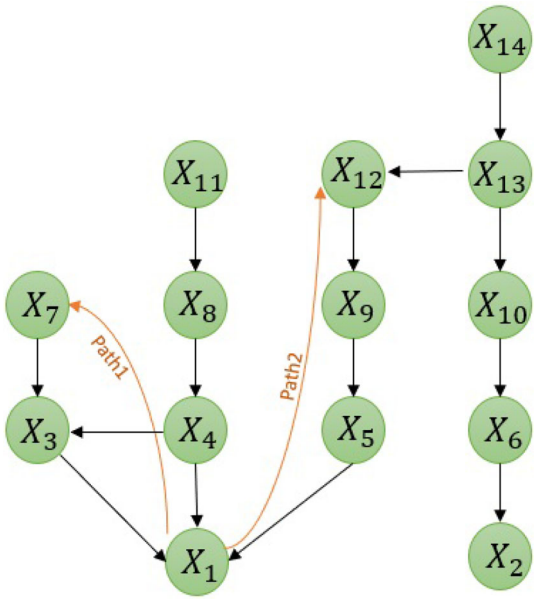

Fig. 5 A simple example of detecting attack paths

$$X_{14} \rightarrow X_{13} \rightarrow X_{12} \rightarrow X_9 \rightarrow X_5 \rightarrow X_1$$
$$X_{11} \rightarrow X_8 \rightarrow X_4 \rightarrow X_3 \rightarrow X_1$$
$$X_{11} \rightarrow X_8 \rightarrow X_4 \rightarrow X_1$$
$$X_7 \rightarrow X_3 \rightarrow X_1$$

Notice that, although there are dependencies between the components as depicted in Fig. 5, not all of them lead to $\mathrm{UE}_{1_{(x_1)}}$. Therefore, by determining the unwanted event and moving backwards, our method prevents blind investigation and can enhance the scalability and efficiency compared to the previous ones.

3.3.2 Compute the risk

The last step of phase III is to compute the risk. The dependency chain illustrated in Fig. 4 clarifies that a critical component in a system will not be affected unless all the pre-conditions of its pertinent dependency chains are fulfilled. Accordingly, to compute the risk of each attack path that may lead to $\mathrm{UE}_{j(X_i)}$, the likelihood of that path being possible to materialize should be calculated. Generally, the probability of an unwanted event occurring (i.e., the Likelihood) multiplied by the magnitude of the consequences (i.e., the Impact) of that event gives an estimate of the risk. Thus, for critical node X_0, risk of materializing an attack path $X_n \rightarrow \cdots \rightarrow X_1 \rightarrow X_0$ with length n is calculated as follows [35]:

$$R_{\mathrm{Path}} = L_{X_n,\ldots,X_0} \times I_{X_1,X_0} = \prod_{i=0}^{n-1} L_{X_i,X_{i+1}} \times I_{X_1,X_0} \qquad (2)$$

where R_{Path} denotes the risk of this attack path. L_i and I_i are the likelihood and impact of targeting X_0, respectively. However, there might be several attack paths toward a critical node X_i and the more paths a target node receives, the higher level of susceptibility and risk it has, as adversaries have several alternatives to target it [36]. To reflect this in computing the risk of each target node X_i, we adopt the concept of risk in [34] and we utilize Eq. 3 below. Here, $P(X_i)$ is the probability of accessing node X_i, which portrays the number of attack paths, and Impact(X_i) denotes the impact resulting when $\text{UE}_{j(X_i)}$ occurs.

$$R(X_i) = P(X_i) \times \text{Impact}(X_i) \tag{3}$$

Due to the fact that identified attack paths for each target node X_i are mutually independent [34], the probability of accessing X_i through at least one of the available attack paths is computed based on Eq. 4.

$$P(X) = 1 - \prod_{i=1}^{k}(1 - p(\text{path}_i)) = 1 - \prod_{i=1}^{k}(1 - L_{X_n,\ldots,X_0}) \tag{4}$$

where $p(\text{path}_i)$ is the likelihood of the attack path i. As Bernsmed et al. [34] asserted, applying this approach to compute the probability of successful attack leads to more realistic results.

It then remains to determine the likelihood and impact. As mentioned earlier, the main objective of the proposed method is to facilitate concurrent analysis of safety and security risks in a CPS. This requires to compute likelihood and impact of an unwanted event based on metrics that contribute to both safety and security. For instance, from the security perspective, an unwanted event might have impact on confidentiality, integrity or availability of a system component and this impact mainly is limited to the system. However, from the safety perspective, this impact includes the environment in which the system is operating and other metrics such as economic effect, public effect and environmental effect should be considered. Therefore, to perform a comprehensive risk assessment for a CPS which encompasses both IT and OT components, we need to assess the impact based on both perspectives. To this end, we leveraged expert knowledge and related methods, mainly stemming from the CVSS Base Metrics [37], and summarized factors affecting the measurement of impact and likelihood in cyber-physical systems as shown in Tables 1 and 2.

Considering both cyber and physical aspects of a CPS, three metrics, namely *Access Vector (AV)*, *Required Knowledge/Skill (KS)* and *External Factors (EF)* are assessed to determine the likelihood. The *Access Vector* metric captures how an attacker can get access to the target component and how difficult this will be. For example, the likelihood of a successful attack when a component can be targeted remotely from outside of the system via the Internet is clearly higher than in the case when the component only can be manipulated via physical access, such as by inserting a USB. The *Required Knowledge/Skill* metric captures the complexity of the attack. This is a significant factor particularly when targeting the OT part in a CPS, as it requires domain knowledge that makes it relatively harder than targeting the IT part. Further, sometimes, in order for an attack to be successful, it must be conducted at a specific time or situation. For instance, in a power plant, improper synchronization can damage a generator only if it happens during a specific time window before the protection device actuates [38]; this will be discussed in some more detail in Sect. 4. A false data injection attack can be seen as another example, in which adversaries need to send false data in a specific time interval to be able to put the system in an unstable situation. Such factors are captured by the *External Factors (EF)* metric. Tables 1 and 2 provide detailed guidance in assigning values to the elements of risk.

The authors in [39] explained that the Likelihood and the Impact score are equal to the average of their constituent metrics. Therefore, by following the approach represented in [39], we compute the Likelihood and the Impact of exploiting a vulnerability or hazard in a dependency chain based on the average of the corresponding metrics defined in Tables 1 and 2 as follows:

$$\text{Likelihood} = \frac{\text{AV} + \text{KS} + \text{EF}}{3} \tag{5}$$

$$\text{Impact} = \frac{\text{Ec} + \text{P} + \text{En} + \text{C} + \text{A} + \text{I}}{6} \tag{6}$$

The scores range from 0 to 1.

It should be noted that, although cyber physical systems are most often composed of numerous components, these components can be classified into a few distinct groups. Based on the data provided by the MITRE Corporation,[1] devices in ICSs from different domains can be classified into seven categories, including (1) Field Controller/RTU/PLC/IED, (2) Safety Instrumented System/Protection Relay, (3) Control Server, (4) Data Historian, (5) Human-Machine Interface, (6) Input/Output Server, and (7) Engineering Workstation. Therefore, by considering the metrics shown in Tables 1 and 2, as well as the above categories of components, stakeholders are able to determine the value of likelihood and impact for each and every one of their system components and type of connection, to create a lookup table toward automating the process of computing risk.

[1] https://attack.mitre.org/techniques/ics/.

Table 1 Likelihood [High(H) = 3, Moderate(M) = 2, Low(L) = 1]

Metric	Category	Description	Value
Access vector (AV)	Remote (R)	Remote access to the vulnerable component or link from outside of the system (Internet)	H
	Adjacent (A)	Access to the vulnerable component or link from a neighbor sub-system/sub-network within the same system	M
	Local-physical (LP)	Physical access to the vulnerable component or link from the same sub-system/sub-network in the same system	L
	Local-cyber (LC)	Cyber access to the vulnerable component or link from the same sub-system/sub-network in the same system	M
Required knowledge/skill (KS)	High	A successful attack requires high level of knowledge and skill	L
	Average	An attacker with average level of knowledge/skill can successfully target the vulnerable component or link	M
	None	Accidental failures or blind attacks affect the the vulnerable component or link	H
External factors (EF)	Required	External Factors such as specific windows of opportunity or privileges are required for a successful attack	L
	None	Attack can be conducted at any time without any pre-requirements	H

Table 2 Impact [High(H) = 3, Moderate(M) = 2, Low(L) = 1, None(N) = 0]

Metric	Description	Values
Economic effect (Ec)	Significance of economic loss and/or degradation of products or services	High (H), Moderate (M), Low (L), None (N)
Public effect (P)	Loss of life, medical illness, serious injury, evacuation	High (H), Moderate (M), Low (L), None (N)
Environmental effect (En)	Effect on the public and the surrounding environment	High (H), Moderate (M), Low (L), None (N)
Confidentiality (C)	Cyber domain (IT assets in a cyber physical system)	High (H), Moderate (M), Low (L), None (N)
	Physical domain (OT assets in a cyber physical system)	
Availability (A)	Cyber domain (IT assets in a cyber physical system)	High (H), Moderate (M), Low (L), None (N)
	Physical domain (OT assets in a cyber physical system)	
Integrity (I)	Cyber domain (IT assets in a cyber physical system)	High (H), Moderate (M), Low (L), None (N)
	Physical domain (OT assets in a cyber physical system)	

3.4 Rank the importance of identified attack paths

As shown in Fig. 1, for every selected node X_i in phase III, all the unwanted events $\mathrm{UE}_{(X_i)}$ are extracted and then the steps shown in the orange block are repeated to find all the related attack paths and compute the corresponding risk. Noticing the feedback loops in Fig. 1, this process continues to compute the risk associated with all identified critical components. Therefore, once the process in phase III is completed, the result should be ranked and critical components with the higher risk value should be prioritized, so that proper action to reduce or manage the risk is taken. Moreover, for each critical component X_i, the result of computing the cybersecurity risks of pertinent attack paths in Phase III will be listed. Paths with higher risk should be prioritized for each critical component.

Apart from the risk associated with each target component X_i, another factor that can help to manage risk to identify and prioritize attack paths is the *perimeter impact*. According to Table 2, perimeter impact indicates the extent to which a failure/malfunctioning of one node can affect the system and, for instance, cause degradation of products/services or even loss of life. The perimeter impact for each attack path can be computed based on the following equation:

$$\mathrm{P} \cdot \mathrm{Impact}_{\mathrm{path}(i)} = \sum_{i=1}^{n} \mathrm{Impact}_{(X_i)} \tag{7}$$

By analyzing the result of Phase III, we can identify common pre-conditions and components that appear in different attack paths. This will guide us toward breaking down the maximum number of attack paths with less effort; consequently, this improves the security of systems.

Reducing the number of attack paths and breaking an attack path are two actions that can directly reduce the risk.

4 Case study

In this section, we demonstrate the use of our proposed method to assess dependency-based safety and security risk based on the system depicted in Fig. 6. As mentioned earlier, the proposed method is domain-agnostic and can be applied in different domains. To demonstrate that, we showcase the workings of our method using a realistic system with a common ICS architecture that can be found in various domains and encompasses both IT and OT assets. To adapt the ICS part and the architecture of the case study to another domain, one would only need to replace the devices in the field network. First, we describe the system architecture and then apply our method.

4.1 Description

Our case study is developed based on the realistic network infrastructures proposed by Homer et al. [27] and Pan et al. [28]. This system represents a simple approximation of a power system that consists of four network zones: a corporate network, a demilitarized zone (DMZ), a field network, and a control network to control critical infrastructure components in the power system. Like all CPSs, in this case study, the control network connects the supervisory control level to lower-level control modules. The corporate network with the control network allows operators to monitor and control the operations from outside of the field network. The DMZ is a separate network segment that connects directly to the firewall and divides the IT and ICS world, for security reasons. The physical process of the system is carried out in the field network. As illustrated in Fig. 6, the field network in the case study is a three-bus two-line transmission system. It is a modified version of the IEEE nine-bus three-generator system [28] that represents the process of generating and transmitting power to the end users (Load) and includes several components.

G1 and G2 are power generators, BR1 through BR4 are breakers and R1 through R4 are relays. Each relay includes integrated phasor measurement unit (PMU) functionality and is able to trip and open the related breaker when a fault occurs on a transmission line. Operators are also able to manually issue commands to each relay to trip and close the corresponding breaker. The data historian and Human Machine Interface (HMI) are among the key ICS components. The data historian stores the logging of all process information within the ICS while the HMI displays reports and status information regarding the state of the processes under control and enables operators to modify control settings and to configure set points [40].

The DMZ, the web server and the VPN server are accessible from the Internet. The VPN server has access to all hosts except those located in the control network, while the web server has only access to the file server through the NFS file-sharing protocol. Accessing the control network from outside would be only allowed from the Citrix server located inside the corporate network. In this case, the Citrix server can only gain access to the data historian. Operators can send commands to the field devices in the field network from the communication server. Figure 6 also depicts potential locations for the presence of insider attackers in the system.

4.2 Risk analysis

As explained in Sect. 3, the first step to accomplish the dependency-based risk analysis is to collect the required data of the system and model the system (phase I). Therefore,

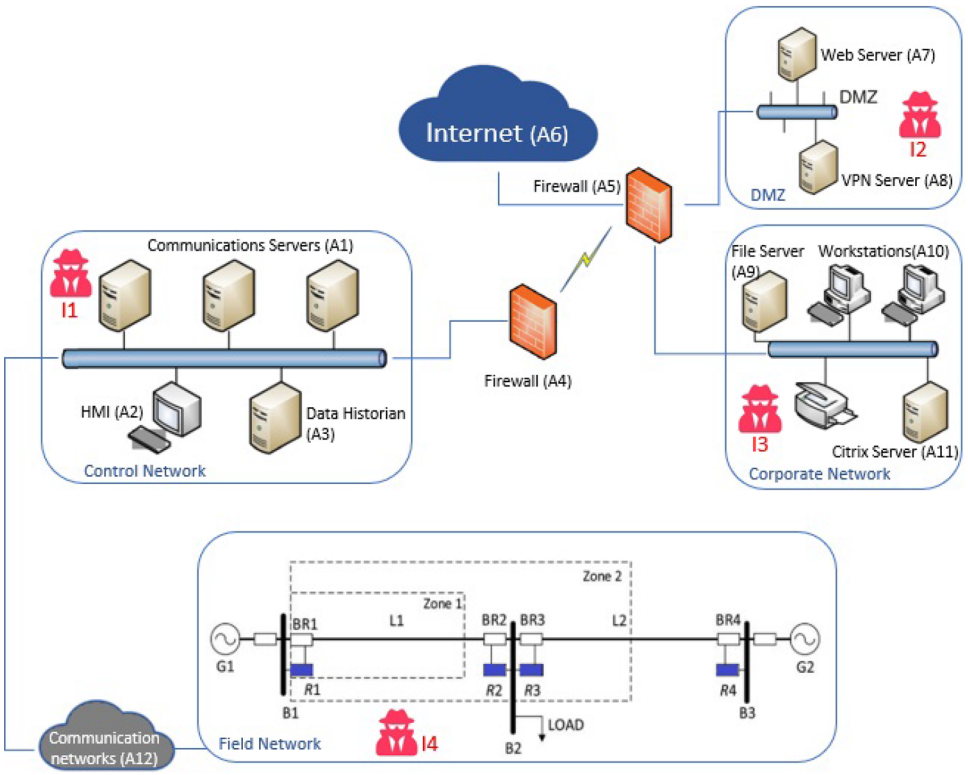

Fig. 6 Graphical representation of the case study

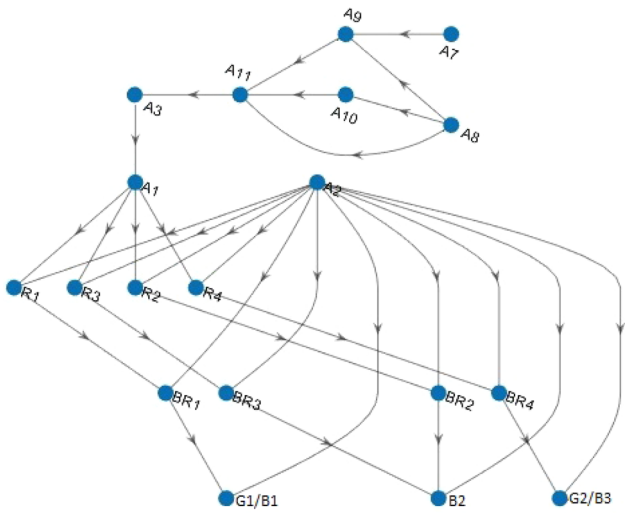

Fig. 7 Digraph of the system

based on the system description and graphical representation of the case study, we provide the digraph of the system as shown in Fig. 7.

Then, we should determine the criticality of the system components following the approach explained in phase II. To this end, the method in [33] is applied to measure the importance of each component from the system level perspective (i.e., C_{sys}). The result of this step is shown in the second column of Table 3. The third column of Table 3 indicates the organizational level criticality of each component which is determined by the expert knowledge here. Finally, by having C_{sys} and C_{Org}, we compute the overall criticality of each component based on Eq. 1 (see Table 3).

According to Table 3, nodes $\{G1, G2, A1, A2, A3, A9, A10, A11\}$ have higher level of criticality compared to other components in the system. Due to the remarkable impact of generators in power systems [38], we select G1 as the target component to run phase III and compute the risk.

Shutting down a generator and damaging it could be seen as two unwanted events. As the former mainly will affect the system, here we choose the latter to investigate how adversaries might be able to cause damage to G1 as one of the system components. Here, we assume that adversaries do not have physical access to G1, as we are interested to analyze the cyber physical attacks and extract related attack paths toward G1. One of the significant reasons that lead to damage to a generator in a power system is the *improper synchronization*.

This could occur due to opening and closing the breaker on the transmission line at a very fast pace which will force the generator to lose synchronization with the transmission grid. When the breaker is opened, the generator is isolated from the grid but due to slow governor response, the mechanical input to the generator does not change immediately. This causes an increase in the generator frequency as compared to the grid frequency. When the breaker is closed out of synchronization or without checking the synchronization requirements, the generator is forced to synchronize; this causes large electrical

Table 3 Criticality value of the system components

Node ID	C_{Sys}	C_{Org}	C_{Total}
B1/G1	0.1693	3	2.1484
BR1	0.357	2	1.6764
R1	0.4916	2	1.811
B2	0.2829	2	1.6023
BR2	0.3423	2	1.6617
R2	0.4761	2	1.7955
BR3	0.3423	2	1.6617
R3	0.4761	2	1.7955
B3/G2	0.1693	3	2.1484
BR4	0.357	2	1.6764
R4	0.4916	2	1.811
A1	1.959	3	3.9381
A2	0.7322	3	2.7113
A3	1.9791	3	3.9582
A7	0.7977	1	1.4574
A8	1.1544	1	1.8141
A9	1.1584	2	2.4778
A10	0.9474	2	2.2668
A11	1.9228	2	3.2422

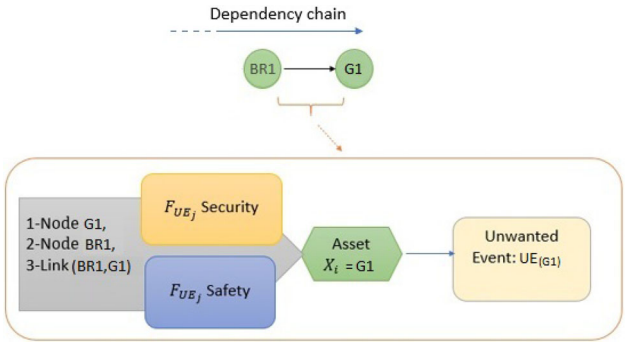

Fig. 8 Checking the first step of the dependency chain for G1

and mechanical transients. The variation of transients due to rapid breaker closing and opening can cause severe physical damage to the generator. Therefore, we consider the improper synchronization as the unwanted event $\text{UE}_{(G1)}$.

Then, we should extract the dependency chains that terminate at G1 and check whether the relations between the nodes in each dependency chain can form attack paths or not. In other words, considering Fig. 4, G1 is placed as the X_i and we investigate the potential cause(s) for $\text{UE}_{(G1)}$ as described in Sect. 3. As shown in Fig. 8, by moving backward from G1, BR1 is the first neighbor node. Considering the functionality of BR1, one can easily find that switching BR1 periodically between the two states, on and off, can lead to the $\text{UE}_{(G1)}$.

Afterward, we consider the attack surface (see Fig. 3) of BR1 to find possible root causes of changing the states of BR1. In the interest of brevity, we only consider the R1 as the neighbor node here. In this case, an intruder (I4) may inject false data into BR1 by leveraging the link $(R1, BR1)$ (this forms path 1 in Table 4), or s/he may take the control of R1 either remotely or manually to send malicious commands to BR1 and change its states between on and off. Path 2 in Table 4 refers to the manual access by I4.

To study the remote access, we should take the next step and identify the attack surface of R1 (i.e., A2 and A1). By following the same approach and leveraging the vulnerabilities described in [27,28], we extract pertinent attack paths that lead to the unwanted event $\text{UE}_{(G1)}$. The results are listed in Table 4. Readers may refer to reference [27] for more details of the vulnerabilities. Note that our main goal here is to show how we can conduct a holistic bottom up risk assessment according to cyber and physical facets of a CPS and available IT/OT knowledge to fill the gap and discover complex cyber physical attacks.

It is noteworthy to heed path 17 in Table 4 as it highlights the necessity of considering both the topological and functional dependencies in risk assessments. As shown in Fig. 6, R1 cooperates in the protection scheme of zone 2 and can trip BR1 when a fault occurs in that zone. Therefore, an attacker may take advantage of this safety scheme to affect G1. In this case, the attacker attempts to emulate a valid fault by sending manipulated data from R3 to the control network and deceive the communication server into sending a trip command to R1 [28,41]. Without considering the functional dependency of A1, this attack path may remain hidden. After identifying the pertinent attack paths, we can determine the likelihood and impact associated with each step of the identified attack paths, based on the guidance in Tables 1 and 2, respectively.

Utilizing a lookup table can facilitate the process of risk assessment. To this end, we develop our lookup table as shown in Table 5. Here, we only consider the components that appear in the identified attack paths. However, in case of a complete risk assessment, this lookup table will be generated for all components, in order to facilitate the computation of likelihood and impact for each system component. Each of the dependency chains shown in Table 5 might appear several times in different attack paths, as will be seen later.

We can then compute the risk and the perimeter impact of each attack path based on Eqs. 2 and 7 as discussed in Sect. 3 (see Table 6). Figure 9 also depicts the risk of each attack path.

As explained in Sect. 3, the risk of $\text{UE}_{(G1)}$ for component $G1$ is computed based on Eq. 3 as follows:

Table 4 Attack paths to G1

No.	Paths
1	$I4 \rightarrow BR1 \rightarrow G1$
2	$I4 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
3	$A6 \rightarrow A7 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
4	$A6 \rightarrow A8 \rightarrow A10 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
5	$A6 \rightarrow A8 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
6	$A6 \rightarrow A8 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
7	$I2 \rightarrow A7 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
8	$I2 \rightarrow A8 \rightarrow A10 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
9	$I2 \rightarrow A8 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
10	$I2 \rightarrow A8 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
11	$I3 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
12	$I3 \rightarrow A10 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
13	$I3 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
14	$I1 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$
15	$I1 \rightarrow HMI \rightarrow R1 \rightarrow BR1 \rightarrow G1$
16	$I1 \rightarrow HMI \rightarrow BR1 \rightarrow G1$
17	$I4 \rightarrow R3 \rightarrow A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$

Table 5 Lookup table for Likelihood and Impact of dependency chains

Step	Likelihood	Impact
$A6 \rightarrow A7$	AV(H)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$A7 \rightarrow A9$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$A9 \rightarrow A11$	AV(M)/KS(M)/EF(L)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$A11 \rightarrow A3$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$A3 \rightarrow A1$	AV(M)/KS(M)/EF(H)	Ec(L)/P(L)/En(L)/C(H)/A(H)/I(H)
$A1 \rightarrow R1$	AV(M)/KS(M)/EF(H)	Ec(M)/P(M)/En(L)/C(M)/A(H)/I(H)
$R1 \rightarrow BR1$	AV(M)/KS(M)/EF(L)	Ec(H)/P(M)/En(M)/C(L)/A(H)/I(H)
$BR1 \rightarrow G1$	AV(M)/KS(M)/EF(L)	Ec(H)/P(H)/En(H)/C(M)/A(H)/I(M)
$A6 \rightarrow A7$	AV(H)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$A7 \rightarrow A10$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(M)/A(M)/I(M)
$A10 \rightarrow A11$	AV(M)/KS(M)/EF(L)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$A8 \rightarrow A11$	AV(M)/KS(M)/EF(L)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$A8 \rightarrow A9$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$I2 \rightarrow A7$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$I2 \rightarrow A8$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$I3 \rightarrow A9$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$I3 \rightarrow A10$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(M)/A(M)/I(M)
$I3 \rightarrow A11$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$I1 \rightarrow A1$	AV(M)/KS(M)/EF(H)	Ec(L)/P(L)/En(L)/C(H)/A(H)/I(H)
$I1 \rightarrow A2$	AV(L)/KS(M)/EF(H)	Ec(H)/P(H)/En(M)/C(H)/A(H)/I(H)
$A2 \rightarrow R1$	AV(M)/KS(M)/EF(L)	Ec(M)/P(M)/En(L)/C(M)/A(H)/I(H)
$A2 \rightarrow BR1$	AV(M)/KS(M)/EF(L)	Ec(H)/P(M)/En(M)/C(L)/A(H)/I(H)
$I4 \rightarrow R1/R3$	AV(L)/KS(M)/EF(L)	Ec(M)/P(M)/En(L)/C(M)/A(H)/I(H)
$I4 \rightarrow BR1$	AV(L)/KS(M)/EF(H)	Ec(M)/P(M)/En(M)/C(M)/A(H)/I(H)
$R3 \rightarrow A1$	AV(M)/KS(M)/EF(L)	Ec(M)/P(M)/En(M)/C(M)/A(M)/I(H)

Table 6 Risk and perimeter impact of identified attack paths

Paths	Likelihood	Perimeter impact	Attack path risk
1	0.0012	0.0723	0.0032
2	0.0013	0.0718	0.0035
3	0.134	0.0659	0.3485
4	0.134	0.0723	0.3485
5	0.0583	0.0723	0.1515
6	0.134	0.0718	0.3485
7	0.1142	0.0659	0.2968
8	0.1142	0.0723	0.2968
9	0.0496	0.0649	0.1291
10	0.1142	0.0645	0.2968
11	0.0496	0.0586	0.1291
12	0.0496	0.0449	0.1291
13	0.0292	0.0488	0.0759
14	0.0055	0.0381	0.0144
15	0.0035	0.0352	0.0092
16	0.0021	0.0244	0.0054
17	0.0053	0.0562	0.0138

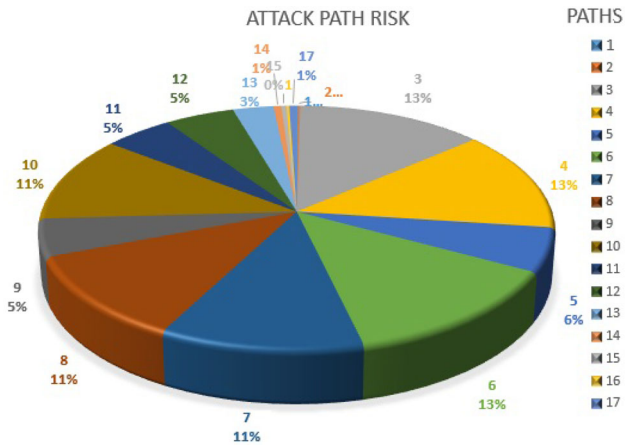

Fig. 9 Risk associated with each attack path

$$
\begin{aligned}
R(G1) &= P(G1) \times \text{Impact}(G1) \\
&= (1 - \prod_{i=1}^{k}(1 - p(\text{path}_i))) \times \text{Impact}(G1) \\
&= (1 - ((1 - 0.0012) \times \cdots \times (1 - 0.0053))) \times 2.6 \\
&= 0.6524 \times 2.6 = 1.6962 \qquad (8)
\end{aligned}
$$

Figure 10 demonstrates the likelihood and perimeter impact of each attack path.

To ensure that the likelihood of each attack path is independent of the length of the dependency chain and the comparison in Fig. 10 is not biased, we divided the value of likelihood of each path by the length of that path (shown in blue color in Fig. 10).

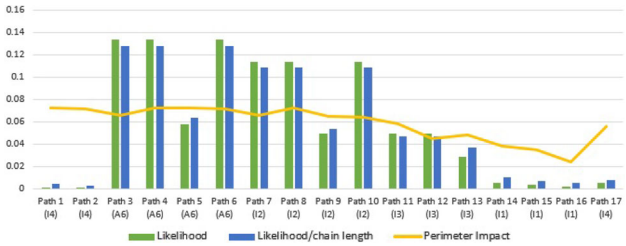

Fig. 10 Likelihood and perimeter impact of identified attack paths

Comparing the identified attack paths based on the likelihood facilitates the identification of the most probable infiltration point and significant attack paths that can lead to the $\text{UE}_{(G1)}$. According to Fig. 10, the likelihood of targeting G1 via A6 and I2 is higher than the rest of the potential entry points. Even within these two groups, the likelihood of path 5 and that of path 9 is significantly low, almost the same as targeting G1 from I3. This information is highly invaluable for risk management in the system.

The advantage of our proposed method will be more clear when it applies to assess the risk of several components in a system. Therefore, we consider relay R1 as the other critical component in the system. In order to calculate the risk of $R1$, we assume that attackers want to modify the settings of relay $R1$. In the system of Fig. 6, relays are configured with a distance protection scheme and changing the settings of a relay can disable the relay function (unwanted event) such that the relay will not trip for a valid fault or a valid command. This can disrupt the smooth operation of the system and cause various types of disturbances in the power system. Attackers can rewrite the settings of a relay either through the HMI on the local network or direct access to the relay. Following the same approach as explained earlier, we extracted the related attack paths to R1 (see Table 7). Then, the likelihood of each path and the impact of targeting $R1$ is calculated and the result is shown in Table 8.

Taking into consideration the identified attack paths, the likelihood and the impact of targeting $R1$, we can compute the risk of targeting $R1$ based on Eq. 3 as follows:

$$
\begin{aligned}
R(R1) &= P(R1) \times \text{Impact}(R1) \\
&= (1 - ((1 - 0.1362) \times \cdots \times (1 - 0.0008))) \times 2.2 \\
&= 0.653 \times 2.2 = 1.4366 \qquad (9)
\end{aligned}
$$

Now, by comparing the risk of $G1$ with that of $R1$ we can clearly understand that, in this system, $G1$ requires higher attention than $R1$ does, which is reasonable as G1 should supply the electrical power to the system. This result is also aligned with the level of criticality of $G1$ in comparison with that of $R1$.

Meanwhile, a closer look at the attack paths in Table 6 reveals that the connections between nodes $A11 \rightarrow A3 \rightarrow$

Table 7 Attack paths to R1

No.	Paths
1	$A6 \rightarrow A7 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
2	$A6 \rightarrow A8 \rightarrow A10 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
3	$A6 \rightarrow A8 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
4	$A6 \rightarrow A8 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
5	$I2 \rightarrow A7 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
6	$I2 \rightarrow A8 \rightarrow A10 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
7	$I2 \rightarrow A8 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
8	$I2 \rightarrow A8 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
9	$I3 \rightarrow A9 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
10	$I3 \rightarrow A10 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
11	$I3 \rightarrow A11 \rightarrow A3 \rightarrow A1 \rightarrow A2 \rightarrow R1$
12	$I1 \rightarrow A2 \rightarrow R1$
13	$I4 \rightarrow R1$

Table 8 Risk and perimeter impact of attack paths toward R1

Paths	Likelihood	Perimeter impact	Attack path risk
1	0.1362	12.6	0.2996
2	0.1362	12.5	0.2996
3	0.0592	1.3	0.1302
4	0.1362	12.6	0.2996
5	0.116	12.6	0.2552
6	0.116	12.5	0.2552
7	0.0504	11.3	0.1109
8	0.116	12.6	0.2552
9	0.0504	11.1	0.1109
10	0.0504	11.1	0.1109
11	0.0297	9.8	0.0653
12	0.0021	5	0.0046
13	0.0008	2.2	0.0018

$A1 \rightarrow R1 \rightarrow BR1 \rightarrow G1$ form the main building block of 11 paths. Notably, the connections between nodes $R1 \rightarrow BR1 \rightarrow G1$ and $BR1 \rightarrow G1$ which appear in another 6 attack paths, are subdivisions of this main building block. This information provides valuable insight for detecting components and corresponding vulnerabilities that frequently appear in different paths; by addressing these, the related attack paths will shrink.

For instance, imagine that we can put in place proper countermeasures to protect the dependency between $BR1$ and $G1$. In this case, none of the identified attack paths can reach $G1$, as adversaries cannot find any vulnerabilities to move from $BR1$ to $G1$ anymore. Although there are still some vulnerabilities and failure modes that attackers can leverage to make their path toward $BR1$, the main goal, i.e., protecting the critical node $G1$, is successfully achieved. Indeed, this satisfies the concept of end-to-end protection that we mentioned earlier, in Sect. 1. Unlike previous risk assessment methods, our proposed method assists system owners and operators to set their objective from the beginning of the analysis and to derive only those paths that can lead to unwanted events affecting the target component. This further helps decision makers to efficiently allocate resources to protect critical components in a system by protecting/removing dependencies existing within the system components that can be leveraged by adversaries to make attack paths toward those critical components.

Here, the risk and the perimeter impact of all attack paths are calculated and these two parameters also help defenders to prioritize the paths with higher risk and impact. In addition to that, the calculation of the overall risk to G1 in case of $\mathrm{UE}_{(G1)}$ facilitates the risk management from a higher level perspective. In other words, while the risk and perimeter impact of each attack path help us to manage the risk associated with a specific unwanted event and its corresponding target component (here $G1$), computing the overall risk of each critical node facilitates the discovery of those unwanted events and pertinent components in a system that require urgent attention and have to be addressed first. Information provided by the proposed risk assessment method can be further utilized to develop a comprehensive risk management method for CPSs; this is part of our future work plans.

5 Discussion

In cyber physical systems, attacks can be carried out from different parts of the system by leveraging flaws and vulnerabilities in cyber components, physical devices, communication links or communication protocols. Therefore, as shown in Sect. 4, discovering and predicting attacks in CPSs require considering both cyber and physical aspects of the systems, as well as the interdependency between them. Considering the physical part of CPSs helps defenders to recognize the intention of attackers and increases the chance of detecting complex cyber physical attacks.

In short, the proposed dependency-based risk assessment has the following characteristics:

- In our proposed method, both the topological and functional dependencies are considered to discover attack paths in a cyber physical system. This means that in the dependency-based risk analysis, the neighbor components with direct connections as well as non-adjacent components that can logically influence the target component due to the functional dependency (i.e., hidden dependency) are studied.
- Unlike previous works which utilize predefined attack vectors and follow a blind investigation to identify target

components in a system, here we apply a backtracking approach which facilitates the exploration of attack scenarios and increases efficiency. This approach also enables operators to view the system from the perspective of attackers and facilitates the detection of new attack paths that might exploit vulnerabilities that have been neglected before and even to discover zero-day vulnerabilities in cyber physical systems.
- Our proposed method is domain-agnostic and can be applied in different CPS domains.
- In our method, the goal of the risk assessment is clear from the beginning, and the risk to each component can be calculated separately. This enhances the efficiency, as unlike previous works, there is no need to investigate the risk of all components/subsystems.
- In this method, risk assessment begins with the most critical components of the system to improve efficiency. To this end, we aggregate the criticality of the system components from both the system and the organizational perspectives.
- By determining the target component corresponding to the unwanted event and moving backwards, the proposed method reduces the investigation of unrelated attack scenarios to zero. That enhances the scalability of the proposed method in comparison with previous ones. The main drawback of the previously developed methods is the speed of growing the number of paths when applied to real-world dimension problems [42] since all the reachable components among the initial components are discovered by moving forward. To extract all attack paths toward a desired component, this process should be repeated for all the components in the system.

6 Conclusion

Unlike previous works, whose main focus has been on the cyber part of CPSs, in this paper both the cyber and physical aspects of a CPS are considered to assess cybersecurity risks. The proposed method facilitates the collaboration between IT and OT operators and, consequently, assists the identification of hard-to-identify and complex attack paths against CPSs. This has been made possible by assessing the risk that the attack paths that lead to a targeted component of a CPS will materialize. Here, an attack path represents violations of security controls that lead to an unwanted event. For every critical component in a system, we extract all the related dependency chains and study potential attack scenarios for each path. For all critical components in a dependency chain, the critical component by itself, its neighbor node, the incoming link are investigated to discover all possible flaws. To increase the efficiency in attack path analysis, a backtracking approach is selected. The workings of the proposed method were showcased using, as an example of a CPS, a realistic power system.

As future work, we plan to present an automated tool to scrutinize possible combinations of vulnerabilities and failure modes of connected components to automatically or semi-automatically generate all attack paths toward target components in a CPS. Besides, the result of the proposed risk assessment method, including the risk and perimeter impact of attack paths, can be further utilized in developing risk management methods for CPSs. We are also interested in studying parallel attack path analysis to investigate its impact on the efficiency of the risk assessment method. The application of the proposed method to CPSs from different domains is also of interest for future work.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital). This work was funded by the Research Council of Norway, through (a) the Joint Indo-Norwegian Project "Cyber-Physical Security in Energy Infrastructure of Smart Cities" (CPSEC), Project No.: 280617; and (b) the SFI "Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS)", Project No.310105.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants performed by any of the authors.

References

1. Alcaraz, C., Lopez, J.: Analysis of requirements for critical control systems. Int. J. Crit. Infrastruct. Prot. **5**(3–4), 137–145 (2012)
2. Abrams, M., Weiss, J.: Malicious control system cyber security attack case study-Maroochy water services, Australia. Tech. Rep, Mitre Corp McLean VA McLean (2008)
3. Chen, T.M., Abu-Nimeh, S.: Lessons from stuxnet. Computer **44**(4), 91–93 (2011)
4. Addeen, H.. H., Xiao, Y., Li, J., Guizani, M.: A survey of cyber-physical attacks and detection methods in smart water distribution systems. IEEE Access **9**, 99 905-99 921 (2021)
5. Castellanos, J. H., Ochoa, M., Zhou, J.: Finding dependencies between cyber-physical domains for security testing of industrial

control systems. In: Proceedings of the 34th Annual Computer Security Applications Conference, pp. 582–594 (2018)
6. Alcaraz, C., Lopez, J., Zhou, J., Roman, R.: Secure SCADA framework for the protection of energy control systems. Concurr. Comput. Pract. Exp. **23**(12), 1431–1442 (2011)
7. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C.: Risk assessment for IoT-enabled cyber-physical systems. In: Advances in Core Computer Science-Based Technologies, pp. 157–173. Springer (2021)
8. Power systems management and associated information exchange—data and communications security—Part 1: Communication network and system security—Introduction to security issues. International Electrotechnical Commission, Geneva, CH, Standard, May (2007)
9. Wang, L., Qu, Z., Li, Z.: The design and implementation of attack path extraction model in power cyber physical system. J. Commun. **11**(9), 834–840 (2016)
10. Chen, Y., Boehm, B., Sheppard, L.: Value driven security threat modeling based on attack path analysis. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), p. 280a. IEEE (2007)
11. Wolf, M., Serpanos, D.N.: Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems. Springer, Berlin (2020)
12. Koscher, K., Savage, S., Roesner, F., Patel, S., Kohno, T., Czeskis, A., McCoy, D., Kantor, B., Anderson, D., Shacham, H.: Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy, pp. 447–462. IEEE Computer Society (2010)
13. Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., Sztipanovits, J., Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In: 2012 5th International Symposium on Resilient Control Systems, pp. 55–62. IEEE (2012)
14. Shakarian, P.: Stuxnet: Cyberwar Revolution in Military Affairs. Technical Reports, Military Academy West Point NY (2011)
15. Kouns, J., Minoli, D.: Information Technology Risk Management in Enterprise Environments. Wiley, Hoboken (2010)
16. Ali, S., Al Balushi, T., Nadir, Z., Hussain, O.: Risk Management for CPS Security, pp. 11–34. Springer International Publishing AG, Cham (2018)
17. Scandariato, R., Wuyts, K., Joosen, W.: A descriptive study of Microsoft's threat modeling technique. Requir. Eng. **20**(2), 163–180 (2015)
18. Freund, J., Jones, J.: Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann (2014)
19. Dorofee, C. A. A.: Managing Information Security Risks: The Octave (SM) Approach (2002)
20. Shevchenko, N., Frye, B. R., Woody, C.: Threat modeling for cyber-physical system-of-systems: methods evaluation. In: Carnegie Mellon University Software Engineering Institute Pittsburgh United..., Technical Reports (2018)
21. Kavallieratos, G., Katsikas, S., Gkioulos, V.: Cybersecurity and safety co-engineering of cyberphysical systems-a comprehensive survey. Future Internet **12**(4), 65 (2020)
22. Lamba, V., Šimková, N., Rossi, B.: Recommendations for smart grid security risk management. Cyber-Phys. Syst. **5**(2), 92–118 (2019)
23. Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V.P.: IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP J. Inf. Secur. **2020**, 1–18 (2020)
24. 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. Sec. **56**, 1–27 (2016)
25. Macher, G., Armengaud, E., Brenner, E., Kreiner, C.: Threat and risk assessment methodologies in the automotive domain. Procedia Comput. Sci. **83**, 1288–1294 (2016)
26. Lyu, X., Ding, Y., Yang, S.-H.: Safety and security risk assessment in cyber-physical systems. IET Cyber Phys. Syst. Theory Appl. **4**(3), 221–232 (2019)
27. Homer, J., Varikuti, A., Ou, X., McQueen, M. A.: Improving attack graph visualization through data reduction and attack grouping. In: International Workshop on Visualization for Computer Security, pp. 68–79. Springer (2008)
28. Pan, S., Morris, T., Adhikari, U.: Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. IEEE Trans. Industr. Inf. **11**(3), 650–662 (2015)
29. Krotofil, M., Kursawe, K., Gollmann, D.: Securing industrial control systems. In: Security and Privacy Trends in the Industrial Internet of Things, pp 3–27. Springer (2019)
30. Skopik, F., Smith, P. D.: Smart grid security: Innovative solutions for a modernized grid. Syngress (2015)
31. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D.-U.: Complex networks: structure and dynamics. Phys. Rep. **424**(4–5), 175–308 (2006)
32. Akbarzadeh, A., Pandey, P., Katsikas, S.: Cyber-physical interdependencies in power plant systems: a review of cyber security risks. In: 2019 IEEE Conference on Information and Communication Technology, pp 1–6. IEEE (2019)
33. Akbarzadeh, A., Katsikas, S.: Identifying critical components in large scale cyber physical systems. In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, pp. 230–236 (2020)
34. Bernsmed, K., Frøystad, C., Meland, P. H., Nesheim, D. A., Rødseth, Ø. J.: Visualizing cyber security risks with bow-tie diagrams. In: International Workshop on Graphical Models for Security, pp. 38–56. Springer (2017)
35. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: Assessing n-order dependencies between critical infrastructures. Int. J. Crit. Infrastruct. 6 **9**(1–2), 93–110 (2013)
36. Akbarzadeh, A., Katsikas, S.: Identifying and analyzing dependencies in and among complex cyber physical systems. Sensors **21**(5), 1685 (2021)
37. FIRST: Common vulnerability scoring system v3.1: User guide. https://www.first.org/cvss/v3.1/user-guide (2019)
38. Zeller, M.: Myth or reality-does the aurora vulnerability pose a risk to my generator? In: 2011 64th Annual Conference for Protective Relay Engineers, pp. 130–136. IEEE (2011)
39. Zinsmaier, S., Langweg, H., Waldvogel, M.: A practical approach to stakeholder-driven determination of security requirements based on the GDPR and common criteria. In: 6th International Conference on Information Systems Security and Privacy, pp. 473–480 (2020)
40. Stouffer, K., Falco, J., Scarfone, K., et al.: Guide to industrial control systems (ICS) security. NIST Spec. Publ. **800**(82), 16 (2011)
41. Hong, J., Nuqui, R.F., Kondabathini, A., Ishchenko, D., Martin, A.: Cyber attack resilient distance protection and circuit breaker control for digital substations. IEEE Trans. Industr. Inf. **15**(7), 4332–4341 (2018)
42. Hong, J. B., Kim, D. S.: Performance analysis of scalable attack representation models. In: IFIP International Information Security Conference, pp. 330–343. Springer (2013)