Attack Path Analysis and Cost-Efficient Selection of Cybersecurity Controls for Complex Cyberphysical Systems

Georgios Spathoulas, Georgios Kavallieratos, Sokratis Katsikas(✉), and Alessio Baiocco

Department of Information Security and Communications Technology, Norwegian University of Science and Technology, Gjøvik, Norway
{georgios.spathoulas,georgios.kavallieratos,sokratis.katsikas, alessio.baiocco}@ntnu.no

Abstract. The increasing integration of information technology with operational technology leads to the formation of Cyber-Physical Systems (CPSs) that intertwine physical and cyber components and connect to each other. This interconnection enables the offering of functionality beyond the combined offering of each individual component, but at the same time increases the cyber risk of the overall system, as such risk propagates between and aggregates at component systems. The complexity of the resulting systems in many cases leads to difficulty in analyzing cyber risk. Additionally, the selection of cybersecurity controls that will effectively and efficiently treat the cyber risk is commonly performed manually, or at best with limited automated decision support. In this paper, we extend our previous work in [1] to analyze attack paths between CPSs on one hand, and we improve the method proposed therein for selecting a set of security controls that minimizes both the residual risk and the cost of implementation. We use the DELTA demand-response management platform for the energy market stakeholders such as Aggregators and Retailers [2] as a use case to illustrate the workings of the proposed approaches. The results are sets of cybersecurity controls applied to those components of the overall system that have been identified to lie in those attack paths that have been identified as most critical among all the identified attack paths.

Keywords: Attack paths · Cyber risk aggregation · Cyber security controls · Power grid

1 Introduction

The increasing proliferation of cyberphysical systems (CPSs) in critical domains including industrial control systems, energy, transportation and healthcare

This paper has been partially funded by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 773960 (DELTA project).

S. Katsikas et al. (Eds.): ESORICS 2021 Workshops, LNCS 13106, pp. 74–90, 2022.
https://doi.org/10.1007/978-3-030-95484-0_5

increases automation and facilitates operations. On the other hand, the increased interoperability and interconnectivity of CPSs increase the attack surface, allowing potential adversaries to perform sophisticated cyber attacks by following attack paths that comprise CPSs as stepping-stones [3].

In particular, the realization of the industry 4.0 paradigm in the power industry increases the interconnectivity and complexity of power grids, rendering them prone to cyber attacks. Indeed, several cyber incidents have been reported in the power industry in the past decade [4], and existing system vulnerabilities in power grids have been identified and analyzed [5].

In an infrastructure comprising networked assets, an attack path describes an ordered sequence of assets that can be used as stepping stones by an adversary aiming to attack one or more assets on the path [6]. By analyzing attack paths, the analysis of the risk propagation and the identification of optimal controls are facilitated. Although the analysis of attack paths is well studied in the literature [7,8], most of the approaches focus on the vulnerabilities of the targeted ecosystem; hence, crucial elements of the cyber risk such as impact and likelihood are not considered.

Contemporary CPS-based infrastructures are characterized by complex information and control flows between their constituent CPSs. These flows can be *direct*, where the components cause immediate change in the node transition, or *indirect*, that can directly or indirectly influence the change in the node transition. These information and control flows provide useful insights to the analysis of cyber risk aggregation, risk analysis, and risk treatment between CPSs. By leveraging different security controls cyber risks are retained, minimized, transferred, or avoided. Although several studies have examined the optimal selection of security controls, most are based on empirical analysis, whose results highly depend on the analyst or domain expert and are, therefore, subjective.

In a previous work of ours [1] we proposed an approach for analyzing risk propagation in complex cyber-physical systems comprising other CPSs as components and leveraged the aggregated risk of the overall system to identify the set of security controls for each component by means of a genetic algorithm approach. In this paper, we extend our previous work in [1] to analyze attack paths between CPSs on one hand, and we improve the method proposed therein for selecting a set of security controls that minimizes both the residual risk and the cost. We have used the DELTA demand-response management platform for the energy market stakeholders such as Aggregators and Retailers [2] as a use case to illustrate the workings of the proposed approaches.

The remainder of this paper is structured as follows: In Sect. 2 we review the related work. In Sect. 3 we briefly review our previous work in [1], so as to both ensure the self-sustainability of this work and to facilitate the assessment of its contribution and of its added value over [1]. Section 4 presents our proposal for analyzing attack paths, and Sect. 5 presents our proposed approach to selecting the optimal set of security controls. Section 6 illustrates the workings of the proposed approaches to the DELTA platform [2]. Finally, Sect. 7 summarizes our conclusions and sets out some future research paths.

2 Related Work

Several approaches have been proposed in the literature to study attack graphs and the analysis of attack paths within IT infrastructures [9]. The ADversary VIew Security Evaluation (ADVISE) meta modeling approach was used in [10] to facilitate the understating of attack paths within cyber-physical systems. A set of algorithms were proposed in [11] to facilitate the analysis of attack paths and to prioritize them taking into account the system's vulnerabilities. A method for analyzing attack paths in CPSs that takes into account the cyber-risk of the involved components was proposed in [6]. Further, an approach for cyber-physical attack path analysis, based on Common Vulnerabilities and Exposures (CVE), and the Common Vulnerability Scoring System (CVSS), and leveraging a threat modeling technique, was proposed in [12]. The propagation of cyber-attacks in a power grid infrastructure was analyzed in [13], taking on the chronological perspective and considering the interrelationship between the grid side and the information side. The analysis focuses on the survivability aspect.

A quantitative risk assessment model that considers the risk propagation among dependent CPSs was proposed in [14]. The risk propagation and prediction have been studied in [15] using Markov chains. The method utilized prediction graph theory and percolation theory to analyze the risk propagation within cyber physical systems in the power domain. The risk propagation between CPSs is examined in [16] based on logical equations and using attack trees; the examined relationships are between parent and children nodes. The risk propagation within a transport network under various types of attacks was analyzed in [17], using the percolation theory. The risk and threat propagation in Unmanned Aerial Vehicles and in particular the aggregation process of the threats from the cyber to the physical domain were discussed in [18].

Cyberattacks cause both safety- and cybersecurity-related damage to CPSs. Accordingly, failure propagation has been also examined in the literature. Specifically, failure propagation in interdependent supply chain networks was studied in [19]; the focus of the analysis was to study the robustness of the supply chain network. Cascading failures within an interdependent network were examined in [20], using an Erdos-Renyi (ER) model, again to study the robustness of the network. In the power domain, cascading failures in a power grid and communication network were analyzed in [21].

3 Background

In [1] we proposed an approach that enables the optimal selection of cybersecurity controls for complex cyberphysical systems, i.e. CPSs that have other CPSs as components. This approach processes the likelihood and impact values for each one of the system's components and, by means of an analysis of how risk propagates through information and control flows components, it calculates the overall, global system risk. It then applies a genetic algorithm workflow that enables the identification of the set of optimal controls for each component.

The identified set minimizes the global system residual risk, and also minimizes the cost of implementation of the controls. The analysis in [1] is conducted on a per-threat basis, for each of the six threats of the STRIDE model. Thus, the approach produces six different control sets, that need to be applied concurrently.

The method assumes a CPS consisting of N interconnected components, each denoted by $c_i,\ i = 1, ...N$. This system can be represented by a directed graph of $N + 1$ nodes, the system itself being one of the nodes, denoted as c_0. The edges of the graph represent information and control flows between the nodes. An edge from node A to node B indicates the existence of either an information flow or a control flow, from A to B. A consequence of the existence of such an edge is that a cybersecurity event at node A affects node B, as well. The *effect coefficient* measures the effect that components may have on each other. Figure 1 depicts a simple graph, where a security event in node A influences node B, while a security event in B influences both nodes A and C. The *total effect coefficient* eff^T_{AB} is computed as a function of eff^I_{AB} and eff^C_{AB} to represent the inverse of the *in degree centrality* measure, as shown in Eq. 1.

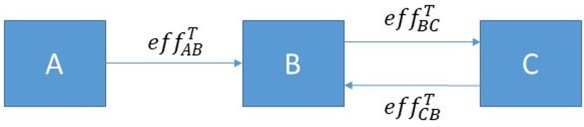

Fig. 1. Effect relationship

$$eff^T_{AB} = f(eff^I_{AB}, eff^C_{AB}), \tag{1}$$

where $eff^I_{AB} = \frac{1}{IDC^I_B}$, $eff^C_{AB} = \frac{1}{IDC^C_B}$.

3.1 Risk Analysis

The risk value R associated with each STRIDE threat $t \in \{S, T, R, I, D, E\}$ for system s is calculated by using the following formulas [22–24]:

$$Impact^s_t = \frac{Damage + Affectedsystems}{2}, \tag{2}$$

$$Likelihood^s_t = \frac{Reproducibility + Exploitability + Discoverability}{3}, \tag{3}$$

$$Risk^s_t = \frac{(Impact^s_t + Likelihood^s_t)}{2}. \tag{4}$$

$Impact^s_t$ describes the effect of a cyber attack realizing specific threat t upon a component s, while $Likelihood^s_t$ describes the probability of the specific threat t being realizing in s.

3.2 Risk Propagation

The *aggregate* risk $R_t^{agg_{c_j}}$ of component c_j is calculated by using Eq. 5.

$$R_t^{agg_{c_j}} = \max(R_t^{dir_{c_j}}, R_t^{prop_{c_j}}), \tag{5}$$

where *direct* risk $R_t^{dir_{c_j}}$ is the risk of c_j without considering the possible connections with other components and it is estimated using Eqs. (2)–(4), while the *propagated* risk $R_t^{prop_{c_j}}$ is calculated considering the connections to other components that c_j has. The fraction of the impact that an event has on any c_k on any path p_l from c_i to c_j is represented by $eff_{p_l}^T$ and is calculated as

$$eff_{p_l}^T = \prod_{i=1}^{j-1} eff_{c_i c_{i+1}}^T. \tag{6}$$

The risk propagated over path p_l, originating at component c_i and terminating at component c_j, is calculated by:

$$R_t^{prop_{c_j}^{p_l}} = \frac{eff_{c_i c_j}^{T_{p_l}} * Impact_t^{c_i} + L_t^{c_i}}{2}. \tag{7}$$

The whole system is described by c_0 and the *global* risk of threat t for the system is calculated by:

$$R_t^s = R_t^{agg_{c_0}} = \max(R_t^{dir_{c_0}}, R_t^{prop_{c_0}}), \tag{8}$$

where the direct risk for the system is not applicable ($R_t^{dir_{c_0}} = 0$) and the propagated risk for the system is calculated as for any other node ($R_t^{prop_{c_0}} = \max_{p_l} R_t^{prop_{c_0}^{p_l}}$), thus

$$R_t^s = \max_{p_l} R_t^{prop_{c_0}^{p_l}} \tag{9}$$

Further details about the method used and the aforementioned equations are omitted in the interest of saving space and can be found in [1].

4 Attack Path Analysis

When the risk of each of a complex CPS components and the propagation of such risk through the interconnection of its components have been analyzed, it is feasible to identify critical attack paths that can potentially induce high risk to the system. Identified critical attack paths can be leveraged by system operators to enhance attack detection measures along the critical paths and to enhance the security of highly interconnected nodes.

The propagation of risk in the system through its components mainly depends on two factors: (a) the structure of the system and (b) the risk to each component. Conceptually, a system can be at high risk because of its components both

because it has high risk components and because there exist high correlation paths along the system structure that may propagate such risk to the overall system.

The approach presented herein analyzes both factors, in order to detect critical attack paths. The approach aims at:

- Detecting critical attack paths according to the relationships (correlation) between components, and
- Prioritizing these paths according to the risk to each component in them.

The first step of the approach can be used to assess the risk propagation potential in a complex cyberphysical system, while the second can be used to gain additional insight, giving more information about the components of the system.

Initially the graph of the system is parsed from the system node backwards, to detect and collect paths that are characterized by a high product of the $eff_{c_i c_j}$ values of the nodes on the path (designated as eff_{path}) along the path. Algorithm 1 outputs a set of critical attack paths, i.e. attack paths that accumulate an eff value larger than a threshold eff_{limit}.

Algorithm 1: Identification of critical attack paths

Result: Critical attack paths *cps*
Function `process_node`(c_j, eff, $path$)**:**
  foreach *edge from* c_i *to* c_j **do**
    if $c_i \notin path$ **then**
      $path = path \cup \{c_i\}$;
      $eff_{path} = eff_{path} * eff_{c_i c_j}$;
      if $eff_{path} > eff_{limit}$ **then**
        $cps = cps \cup \{path\}$;
        $process\_node(c_i, eff_{path}, path)$;
      end
    end
  end
$cps = \{\}$;
`process_node`(c_0, *1*, $\{c_0\}$);

The second step of the approach, described in Algorithm 2, prioritizes the attack paths that were identified in step 1, by considering the risk of each component in each path.

Algorithm 2: Prioritization of critical attack paths

Result: Prioritized critical attack paths *pri_cps*
Function `calc_risk(`*path*`):`
  $R = \frac{L_{path[0]}+I_{path[0]}}{2}$;
  $i = 0$;
  $eff = 1$;
  while $i < path_{length}$ **do**
    $i = i + 1$;
    $eff = eff * eff_{path[i],path[i-1]}$;
    $R = max(R, \frac{L_{path[i]}+I_{path[i]}*eff}{2})$
  end
  return R;
Function `select_paths(`*cps*`):`
  foreach *path in cps* **do**
    $R_{path} = calc\_risk(path)$;
    if $R_{path} > R_{path}^{limit}$ **then**
      $pri\_cps = pri\_cps \cup \{path\}$;
    end
  end
$pri\_cps = \{\}$;
`select_paths();`

5 Optimal Control Set Selection

5.1 Cybersecurity Controls

The proposed approach requires a pool of controls that are appropriate for the targeted system. The effectiveness of the controls depends on the effect that each control has per threat and per component c_i. The effect influences the values of $Impact_t^{c_i}$ and $Likelihood_t^{c_i}$ and hence the cyber-risk to the components and to the overall system.

An important feature of each control m is the cost $Cost_m$ of its implementation. For a system with N components and a list with M controls with the cost vector $C = [cost_1, cost_2, ..., cost_M]$, the following binary matrix AC compactly depicts the applied controls throughout the system:

$$AC = \begin{bmatrix} ac_{1,1} & ac_{1,2} & ... & ac_{1,N} \\ ac_{2,1} & ac_{2,2} & ... & ac_{2,N} \\ ... & ... & ... & ... \\ ac_{M,1} & ac_{M,2} & ... & ac_{M,N} \end{bmatrix}, \tag{10}$$

where

$$ac_{i,j} = \begin{cases} 0, \textit{if control } i \textit{ is not applied to component } j \\ 1, \textit{if control } i \textit{ is applied to component } j \end{cases}. \tag{11}$$

The total cost TC_{AC} of the applied controls solution AC is $TC_{AC} = AC * C$.

5.2 Selection of the Optimal Set

The approach in [1] produced a separate optimal set of controls for each STRIDE threat, and did not take into account that those controls could be possibly combined, to achieve a more efficient, from a global perspective, solution. For example the application of a single control to a specific component could result in reduction of the overall system risk for more than one threats, but this was not taken into account.

To remedy this, the present work proposes a cascading application of the genetic algorithm approach, in which each step (for each different threat) takes as granted that the controls that have been identified in the previous steps are, indeed, implemented. This approach enables the elicitation of controls that are effective for more than one threats. Therefore the selection is more efficient with respect to the global implementation cost. The proposed scheme supports the identification of the set of controls that minimizes the risk over all threats and the implementation cost for the system as a whole.

The concept upon which the approach is based is depicted in Fig. 2. After applying the genetic algorithm for each threat, the resulting controls are fixed in the set of available controls that is used as input for the rest of the threats. After all threats have been analyzed, the resulting controls are being unified as the optimal set of cyber-security controls for the system as a whole.

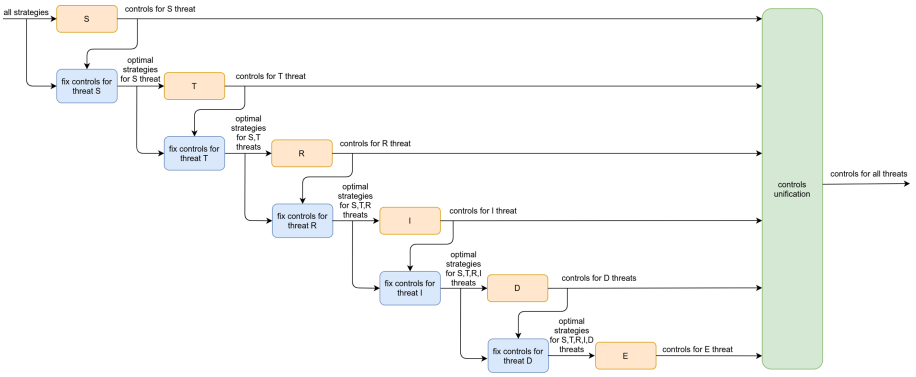

Fig. 2. Cascading GA process

The above methodology uses a global AC^* matrix, which has fixed values for the combinations of components/controls that have been defined for all threats. Specifically, the AC^* matrix is an instance of the AC matrix defined in Eq. 10, each element $ac_{i,j}$ of which is related to the application of control i to component j and is:

– either a binary variable whose value can be set according to risk reduction and application cost.

– or a fixed value variable (equal to 1) if control i has been decided to be applied to component j for countering a threat analyzed previously.

This approach fixes the application of controls to components between different threats of the STRIDE model. It will only allow controls to be considered for threat T only if these further reduce the risk for threat t_i, given that controls decided for each threat $t_j, i > j$ have already been applied.

The proposed methodology is significantly more efficient in terms of application cost, while it retains residual risk on a similar level as the per threat analysis in [1].

6 DELTA System Use Case

6.1 The DELTA System

DELTA is the short title of the EU-funded H2020 R&D project "Future tamper-proof Demand rEsponse framework through seLf-configured, self-opTimized and collAborative virtual distributed energy nodes"[1]. DELTA has developed a demand-response management platform that distributes parts of the Aggregator's intelligence into lower layers of its architecture, in order to establish a more easily manageable and computationally efficient Demand-Response (DR) solution. This approach aims to introduce scalability and adaptivity into the Aggregator's DR toolkits; the DELTA core engine is able to adopt and integrate multiple strategies and policies provided from its administrative stakeholders, making it an authentic modular and future-proof solution.

An overview of the DELTA architecture can be found in [25] and a detailed description of it in [26]. A graph-based representation of the DELTA architecture is depicted in Fig. 3. The nodes of the graph represent DELTA building blocks, as follows:

Node S - System: it represents the whole DELTA system.

Node D - DVN: DVN stands for "DELTA Virtual Network", a virtual layer that clusters consumers/prosumers/producers sharing key characteristics, such as a similar consumption/generation pattern, kind of (smart) contract, existence (or not) of Energy Storage Systems (ESS); the disposition to participate into DR strategies; or their resulting behavior during a DR signal based on the award system, following the guidelines/strategies provided by the Aggregator.

Node F - FEID: FEIDs are actual devices which are connected to smart meters to measure energy-related data. Through an intelligent lightweight toolkit they compute real-time flexibility to provide as input to the DVN. FEIDs provide aggregated metering from multiple IoT devices that are connected to customer assets, and they report issuance and interpretation of OpenADR-based DR request signals.

[1] https://www.delta-h2020.eu/.

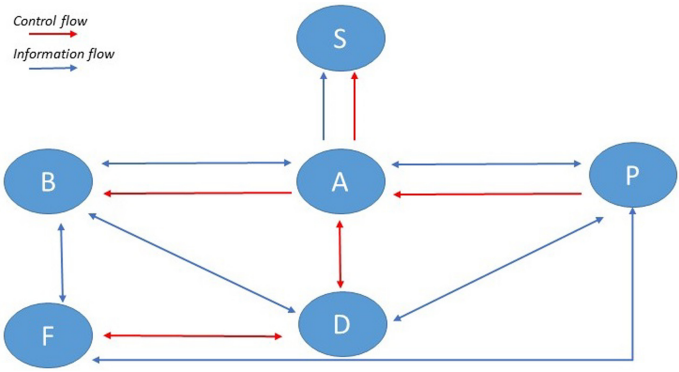

Fig. 3. DELTA components

Node P - P2P Network: it represents the communications backbone of the entire DELTA framework. The use of the peer-2-peer network guarantees a certain resilience to attacks/malfunctions, and greater modularity in the management of the tasks performed by each of the entities that make up DELTA. DELTA's P2P network allows the use of OpenADR to interface with FEIDS in order to manage DR requests and uses the OpenFIRE as a communication broker, in addition to implementing Access Controls security.

Node A - Aggregators: Aggregators are entities, generally TSOs or DSOs, which supply energy to users, but also acquire it from users known as *prosumers*. They balance network loads through DR or other traditional load shedding methods, and they collect data from smart meters for statistical purposes, control and pricing.

Node B - Blockchain: it is a block used to ensure the security of the energy information exchange within the DELTA energy network, enabling both energy data traceability and secure access for stakeholders. Technologies employed include certificates, blockchain, smart contracts, and state of the art security and privacy algorithms.

6.2 Risk Analysis

In order to apply the proposed approach, a risk analysis of the targeted system is required. To this end, the STRIDE [27] and DREAD [22] methodologies have been used. The *impact* and *likelihood* values for each of the STRIDE threats have been estimated and are depicted in Table 1. Each line of Table 1 represents one of the STRIDE threats, indicated by the corresponding initial (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privileges). Each column of Table 1 represents an individual DELTA component as described in Sect. 6.1. The values in the cells are the corresponding impact and likelihood values per STRIDE threat and per individual component; these have been calculated by means of Eqs. (2) and (3), respectively. These values

are subsequently used as input to Algorithm 2, to calculate the aggregate risk of each component. Table 2 depicts the values of the $eff_{c_i c_j}$ coefficients for all pairs of components.

Table 1. Initial security analysis

	System	Impact					System	Likelihood				
		FEID	DVN	Aggregator	P2PNetwork	Blockchain		FEID	DVN	Aggregator	P2PNetwork	Blockchain
S	0	1.5	2.5	2.5	2.5	1.5	0	2	1.66	2	1.66	1.66
T	0	1.5	2	2.5	2.5	1	0	2	1.33	1.66	2	1
R	0	1.5	1.5	2.5	2.5	1	0	2	1.33	2	2	1
I	0	1	1.5	1.5	2	1	0	1.66	1	1.66	1.33	1.66
D	0	2	3	1.5	3	2	0	2.33	1.66	2.33	3	1.66
E	0	1.5	2	2.5	2.5	1	0	1.66	1.66	2	1.66	1

Table 2. Effect coefficients

	System	FEID	DVN	Aggregator	P2PNetwork	Blockchain
System	0	0	0	0	0	0
FEID	0.3	0	0.1	0	0.3	0.3
DVN	0	0.2	0	0.2	0.2	0.2
Aggregator	0	0	0.1	0	0.2	0.2
P2PNetwork	0.3	0.3	0.3	0.3	0	0
Blockchain	0	0.3	0.3	0.3	0	0

6.3 Attack Path Analysis

The proposed attack path analysis methodology was subsequently applied to the DELTA system. The results of the first step of the approach (identification) are depicted in Table 3. Each line in Table 3 contains the path ID, the attack path, and the corresponding value of eff_{path}, calculated using the values of the effect coefficients in Table 2. The paths that can potentially enable the propagation of high risk to the system (hence they are the most critical) are the ones that are characterized by the highest eff_{path} values; these are the first five paths of Table 3.

The results of the second step of the approach (prioritization) are depicted in Table 4. Each line in Table 4 contains the path ID, the attack path, and the corresponding value of the cyber-risk of the path, taken to be the highest among the risks of the nodes in the path, as in [1].

6.4 Selection of the Optimal Security Controls

In order to select the set of optimal controls we applied both the approach in our previous work [1] and the one proposed herein, to validate the claim that the

Table 3. List of attack paths

Path ID	Affected CPSs	eff_{path}
1	FEID → System	**0.3**
2	P2P Network → System	**0.3**
3	P2P Network → FEID → System	**0.09**
4	Blockchain → FEID → System	**0.09**
5	FEID → P2P Network → System	**0.09**
6	DVN → FEID → System	0.06
7	DVN → P2P Network → System	0.06
8	Aggregator → P2P Network → System	0.06
9	Blockchain → FEID → P2P Network → System	0.027
10	P2P Network → DVN → FEID → System	0.018
11	Blockchain → DVN → FEID → System	0.018
12	DVN → P2P Network → FEID → System	0.018
13	Aggregator → P2P Network → FEID → System	0.018
14	DVN → Blockchain → FEID → System	0.018
15	Aggregator → Blockchain → FEID → System	0.018

latter is more effective and that it results in a larger ratio of reduction of risk vs control implementation cost. The controls in the NIST guidelines for Industrial Control Systems security [28] have been used as the pool of available controls. As in [1], the effectiveness and the cost of each security control are estimated on the basis of its applicability, the extent to which it reduces the impact or/and the likelihood, and the resources needed to implement it. Table 5 presents the results obtained with the initial method [1], whilst Table 6 presents the results obtained with the improved method proposed herein.

From these results it is obvious that the improved method proposed herein can produce the same effect with respect to residual risk for all threats, whilst it reduces the application cost from 70 to 61. In other words, the improved method increases the risk reduction per application cost ratio by 12.9%. We note that the selected controls differ between the two executions, because of the different approach used, but also because there exist multiple controls that have the same effect, and it is normal for the proposed (randomized search) approach to randomly choose among those in each run.

Table 4. Prioritized attack paths per threat and risk level

	Attack path	Cyber risk
Path ID	Spoofing	
2	P2P Network → System	1.45
1	FEID → System	1.225
3	P2P Network → FEID → System	1.135
4	Blockchain → FEID → System	1.135
Path ID	Tampering	
2	P2P Network → System	1.375
1	FEID → System	1.225
3	P2P Network → FEID → System	1.1125
8	Aggregator → P2P Network → System	1.09
Path ID	Repudiation	
2	P2P Network → System	1.375
1	FEID → System	1.225
3	P2P Network → FEID → System	1.1125
8	Aggregator → P2P Network → System	1.09
Path ID	Information disclosure	
1	FEID → System	1.54
2	P2P Network → System	1.45
5	FEID → P2P Network → System	1.2775
6	DVN → FEID → System	1.24
Path ID	Denial of service	
1	FEID → System	1.45
2	P2P Network → System	1.45
3	P2P Network → FEID → System	1.135
5	FEID → P2P Network → System	1.135
Path ID	Elevation of privileges	
2	P2P Network → System	1.615
1	FEID → System	1.465
3	P2P Network → FEID → System	1.3
5	FEID → P2P Network → System	1.255

Table 5. Optimal cybersecurity controls - per threat

	Initial global risk	Cybersecurity controls	Residual global risk	Overall cost
Component	Spoofing			
Aggregator	1.3	Awareness and training	0.864	14
P2P		Awareness and training		
DVN		Security assessment and authorization		
BC		Security assessment and authorization		
FEID		Configuration management		
Component	Tampering			
BC	1.3	Access control	0.65	17
P2P		Security assessment and authorization		
Aggregator		Risk assessment		
FEID		System and services acquisition		
DVN		System and communications protection		
Component	Repudiation			
DVN	1.3	Security assessment and authorization	0.864	6
Aggregator		Security assessment and authorization		
P2P		Security assessment and authorization		
FEID		Maintenance		
Component	Information disclosure			
BC	1.514	Privacy controls	0.65	17
FEID		Security assessment and authorization		
P2P		Planning		
DVN		System and services acquisition		
Aggregator		System and services acquisition		
DVN		System and information integrity		
Component	Denial of service			
FEID	1.3	Security assessment and authorization	0.65	7
DVN		Security assessment and authorization		
Aggregator		Security assessment and authorization		
P2P		Risk assessment		
BC		System and communication protection l		
Component	Elevation of privileges			
P2P	1.514	Audit and accountability	1.079	9
BC		Audit and accountability		
DVN		Security assessment and Authorization		
Aggregator		Security assessment and authorization		
FEID		Risk assessment		
				Overall cost
				70

Table 6. Optimal cybersecurity controls - global

	Initial global risk	Cybersecurity controls	Residual global risk	Cost per threat
Component	Spoofing			
P2P	1.3	Awareness and training	0.864	16
DVN		Configuration management		
FEID		Identification and authentication		
BC		Identification and authentication		
Aggregator		Incident response		
Component	Tampering			
P2P	1.3	Audit and accountability	0.65	20
DVN		Security assessment and authorization		
FEID		Configuration management		
Aggregator		Identification and authentication		
Aggregator		Risk assessment		
BC		System and communications protection		
Component	Repudiation			
Aggregator	1.3	Audit and accountability	0.864	3
P2P		Audit and accountability		
FEID		Configuration management		
DVN		Configuration management		
Component	Information disclosure			
BC	1.514	Access control	0.65	13
Aggregator		Audit and accountability		
FEID		Configuration management		
DVN		Configuration management		
P2P		Maintenance		
FEID		Risk assessment		
DVN		System and services acquisition		
Component	Denial of service			
P2P	1.3	Awareness and training	0.65	3
P2P		Audit and accountability		
FEID		Security assessment and authorization		
DVN		Security assessment and authorization		
FEID		Configuration management		
DVN		Configuration management		
Aggregator		Incident response		
BC		System and communications protection		
Component	Elevation of privileges			
P2P	1.514	Audit and accountability	1.079	6
BC		Audit and accountability		
DVN		Security assessment and authorization		
FEID		Configuration management		
DVN		Configuration management		
FEID		Contingency planning		
Aggregator		Incident response		
				Overall cost
				61

7 Conclusions

The increasing dependence of critical infrastructures, such as power grids, on interconnected CPSs increases the attack surface and makes them prone to

cyberattacks. The analysis of attack paths facilitates the comprehensive understanding of the attack propagation towards the selection of the most appropriate security controls. By leveraging the proposed methods for attack path analysis and optimal control selection, all the elements of cyber risk can be studied, towards defining a security architecture. As future work we intend to develop an automated tool that supports the proposed methods. Additionally, the utilization of the proposed approaches in several instances of the DELTA system will facilitate the development of secure power grids.

References

1. Kavallieratos, G., Spathoulas, G., Katsikas, S.: Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. Sensors **21**(5), 1691 (2021)
2. Tsolakis, A.C., et al.: A secured and trusted demand response system based on blockchain technologies. In: 2018 Innovations in Intelligent Systems and Applications (INISTA), pp. 1–6 (2018)
3. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J.: A survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor. **20**(4), 3453–3495 (2018)
4. Macola, I.G.: The five worst cyberattacks against the power industry since 2014 (2020). https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/. Accessed 20 July 2021
5. Vellaithurai, C., Srivastava, A., Zonouz, S., Berthier, R.: CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures. IEEE Trans. Smart Grid **6**(2), 566–575 (2014)
6. Kavallieratos, G., Katsikas, S.: Attack path analysis for cyber physical systems. In: Katsikas, S., et al. (eds.) CyberICPS/SECPRE/ADIoT 2020. LNCS, vol. 12501, pp. 19–33. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64330-0_2
7. Xie, A., Cai, Z., Tang, C., Hu, J., Chen, Z.: Evaluating network security with two-layer attack graphs. In: 2009 Annual Computer Security Applications Conference, pp. 127–136. IEEE (2009)
8. Ou, X., Boyer, W.F., McQueen, M.A.: A scalable approach to attack graph generation. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 336–345 (2006)
9. Lippmann, R.P., Ingols, K.W.: An annotated review of past papers on attack graphs (2005)
10. Cheh, C., Keefe, K., Feddersen, B., Chen, B., Temple, W.G., Sanders, W.H.: Developing models for physical attacks in cyber-physical systems. In: Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and Privacy, pp. 49–55 (2017)
11. Mouratidis, H., Diamantopoulou, V.: A security analysis method for industrial internet of things. IEEE Trans. Industr. Inf. **14**(9), 4093–4100 (2018)
12. Stellios, I., Kotzanikolaou, P., Grigoriadis, C.: Assessing IoT enabled cyber-physical attack paths against critical systems. Comput. Secur. **107**, 102316 (2021)
13. Liang, X., Wu, Y., Ni, M., Li, M.: Survivability index and evaluation framework for cyber physical power systems. In: 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1–5. IEEE (2020)

14. Malik, A.A., Tosh, D.K.: Quantitative risk modeling and analysis for large-scale cyber-physical systems. In: 2020 29th International Conference on Computer Communications and Networks (ICCCN), pp. 1–6. IEEE (2020)
15. Qu, Z., et al.: Power cyber-physical system risk area prediction using dependent Markov chain and improved grey wolf optimization. IEEE Access **8**, 82844–82854 (2020)
16. Potteiger, B., Martins, G., Koutsoukos, X.: Software and attack centric integrated threat modeling for quantitative risk assessment. In: Proceedings of the Symposium and Bootcamp on the Science of Security, pp. 99–108 (2016)
17. Guo, J., Xu, J., He, Z., Liao, W.: Research on risk propagation method of multimodal transport network under uncertainty. Physica A **563**, 125494 (2021)
18. Guo, R., Tian, J., Wang, B., Shang, F.: Cyber-physical attack threats analysis for UAVs from cps perspective. In: 2020 International Conference on Computer Engineering and Application (ICCEA), pp. 259–263. IEEE (2020)
19. Tang, L., Jing, K., He, J., Stanley, H.E.: Complex interdependent supply chain networks: cascading failure and robustness. Physica A **443**, 58–69 (2016)
20. Chattopadhyay, S., Dai, H.: Estimation of robustness of interdependent networks against failure of nodes. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2016)
21. Parandehgheibi, M., Modiano, E.: Robustness of interdependent networks: the case of communication networks and the power grid. In: 2013 IEEE Global Communications Conference (GLOBECOM), pp. 2164–2169. IEEE (2013)
22. Microsoft: Chapter 3 - threat modeling (2010). https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN
23. Langweg, H., Zinsmaier, S.D., Waldvogel, M.: A practical approach to stakeholder-driven determination of security requirements based on the GDPR and common criteria. In: Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), pp. 473–480 (2020)
24. Kavallieratos, G., Katsikas, S.: Managing cyber security risks of the cyber-enabled ship. J. Marine Sci. Eng. **8**(10), 768 (2020)
25. Patsonakis, C., Terzi, S., Moschos, I., Ioannidis, D., Votis, K., Tzovaras, D.: Permissioned blockchains and virtual nodes for reinforcing trust between aggregators and prosumers in energy demand response scenarios. In: 2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I CPS Europe), pp. 1–6 (2019)
26. Psara, K., et al.: DELTA Overall Framework Architecture v2 (2020). https://www.delta-h2020.eu/wp-content/uploads/2020/06/DELTA_D1.6_Final.pdf
27. Shostack, A.: Threat Modeling: Designing for Security. Wiley, New York (2014)
28. Stouffer, K., Pillitteri, V., Marshall, A., Hahn, A.: Guide to industrial control systems (ICS) security. NIST Spec. Publ. **800**(82), 247 (2015)