A Methodology for Monitoring and Control Network Design

István Kiss(✉) and Béla Genge

"Petru Maior" University of Tîrgu Mureş, Tîrgu Mureş, Romania
istvan.kiss@stud.upm.ro, bela.genge@ing.upm.ro

Abstract. The accelerated advancement of Industrial Control Systems (ICS) transformed the traditional and completely isolated systems view into a networked and inter-connected "system of systems" perspective. This has brought significant economical and operational benefits, but it also provided new opportunities for malicious actors targeting critical ICS. In this work we adopt a Cyber Attack Impact Assessment (CAIA) technique to develop a systematic methodology for evaluating the risk levels of ICS assets. The outcome of the risk assessment is integrated into an optimal control network design methodology. Experiments comprising the Tennessee Eastman chemical plant, the IEEE 14-bus electricity grid and the IEEE 300-bus New England electricity grid show the applicability and effectiveness of the developed methodology.

Keywords: Industrial Control Systems · Impact assessment
Cyber attack · Optimal network design · Risk assessment

1 Introduction

The pervasive adoption of commodity, off-the-shelf Information and Communication Technologies (ICT) reformed the architecture of ICS. This has brought numerous benefits including the reduction of costs, greater flexibility, efficiency and interoperability between components. However, the massive penetration of ICT hardware and software into the heart of modern ICS also created new opportunities for malicious actors and facilitated the adoption of traditional cyber attack vectors for the implementation of a new breed of *cyber-physical* attacks. These represent a more sophisticated class of attacks where the characteristics of the cyber and the physical dimensions are exploited by the adversary in order to cause significant damages to the underlying physical process. Stuxnet [4], Flame [5] and Dragonfly [18] represent only a fraction from the number of threats showcasing the impact of exploiting ICT vulnerabilities in ICS.

As a response to these events, a significant body of research focused on the identification of critical ICS assets and on improving the security of these kind infrastructures [13,15–17]. However, previous studies do not address the dynamic behavior of ICS, the complexity of ICS, the existing inter-dependencies

G. Havarneanu et al. (Eds.): CRITIS 2016, LNCS 10242, pp. 111–122, 2017.
https://doi.org/10.1007/978-3-319-71368-7_10

between ICT and the physical process. Furthermore, the output of risk assessment methodologies is not integrated into a network design framework. Therefore, in this work we extend our solutions given in [12] by developing a framework for assessing the impact of cyber attacks on ICS and for the optimal design of ICS networks. The framework adopts a Cyber Attack Impact Assessment (CAIA) methodology in order to evaluate the risk levels associated to each ICS asset. The output of this approach is then used in an Integer Linear Programming (ILP) problem for optimally designing control networks. The aim of the optimization is to minimize the distance between concentrator nodes and end devices, as well as to maintain link capacity and security level constraints. As a result, the ICS designed according to the proposed framework ensures the protection of critical devices as well as their low installation and operational costs. The proposed framework is evaluated by means of extensive experiments including the Tennessee Eastman chemical plant (TEP) [6], the IEEE 14-bus electrical grid, the IEEE 300-bus electrical grid and various attack scenarios.

The remaining of this paper is structured as follows. Section 2 provides a brief overview of the related research. The description of the risk assessment technique is given in Sect. 3, which is followed by the network design technique in Sect. 4, experimental assessment in Sect. 5, and conclusions in Sect. 6.

2 Related Work

First, we investigate related cyber attack impact assessment techniques, such as the work of Kundur *et al.* [13]. Here, the authors proposed a graph-based model to evaluate the influence of control loops on a physical process. Differently, in [16], Sgouras *et al.* evaluated the impact of cyber attacks on a simulated smart metering infrastructure. The experiments implemented disruptive Denial of Service attacks against smart meters and utility servers, which caused severe communication interruptions. In a different work, Sridhar and Govindarasu [17] showed that cyber attacks may significantly impact power system stability by causing severe decline of system frequency. Bilis *et al.* in [2] proposed a complex network theory-based assessment methodology to show the individual importance of electric buses in power systems. Next, we briefly mention the related network design techniques. Carro-Calvo *et al.* [3] developed a genetic algorithm-based optimal industrial network partitioning, which maximized intra-network communications and minimized inter-network data transfers. Zhang *et al.* [19,20] elaborated a network design problem, which reduces network delays. In [9] Genge and Siaterlis revealed that the impact of local actuation strategies to other controllers should also be considered in network design procedures. Another work of Genge *et al.* in [8] proposed a Linear Programming-based network design optimization problem that accounts for the presence of primary and secondary networks, as well as for the capacity of links and devices, the security and real-time traffic requirements.

In contrast with the aforementioned techniques, the primary contribution of this work is that it delivers a complete framework for assessing the impact of cyber attacks on ICS, for establishing concrete risk levels and for designing ICS. This represents a significant contribution over the state of the art since it closes the gap between risk assessment and security-aware network design.

3 Asset Risk Assessment in ICS

The architecture of modern ICS is structured according to two different layers: (i) the physical layer, which encompasses a variety of sensor, actuator, and hardware devices that physically perform the actions on the system; (ii) and the cyber layer, which encompasses all the ICT hardware and software needed to monitor the physical process and to implement complex control loops. From an operational point of view, hardware controllers, i.e., Programmable Logical Controllers (PLC), receive data from sensors, elaborate local actuation strategies, and send commands to the actuators. These hardware controllers also provide the data received from sensors to Supervisory Control and Data Acquisition (SCADA) servers and eventually execute the commands that they receive. Hereinafter, the devices that acquire and transmit data from multiple sources are referred to as Concentrator Nodes (CN).

3.1 Overview of the CAIA Approach

The cyber attack impact assessment (CAIA) technique proposed in our previous work [10] adopts a procedure inspired from the field of System Dynamics [7]. According to [7], a change in the systems' behavior is the result of interventions induced by control variables. In CAIA this effectively translates to the reduction of the state-space and more specifically of the number of variables and attacks that need to be evaluated. At the core of CAIA is a technique that records the *behavior* of complex physical processes in the presence of accidental or deliberate interventions, e.g., faults, events, and cyber attacks. Essentially, the cyber attack impact assessment procedure calculates the cross co-variance of observed variables before and after the execution of a specific intervention. Accordingly, an instance of CAIA results in an impact matrix denoted by C which columns correspond to observed variables and the rows to control variables. Therefore, the C impact matrix enables a detailed impact assessment in various scenarios by providing answers to research questions such as measuring how the intervention on the i-th control variable affects the j-th observed variable. The next section employs the impact matrix as the input to the *risk assessment procedure*. More details about the CAIA procedure are given in [10].

3.2 Risk Assessment Based on the Impact Measures

The CAIA procedure delivers relative impact values for one specific type of attack. Therefore, the risk assessment expands the CAIA approach and combines the output of multiple executions of CAIA for different attacks. First we define $A = \{1, 2, ..., \iota, ...\alpha\}$ as the set of attack types. We use C^{ι}_{ij} to denote the impact matrix values such that C_{ij} is the calculated impact for the ι-th attack type ($\iota \in A$). Next, as a pre-processing step, a PCA (Principal Component Analysis) based weighting technique [14] is used to combine the results of impact assessments of multiple attack types and to construct a *severity* matrix Ω used later in the calculation of risk values. The values of this matrix denoted by $\omega_{i\iota}$, represent the severity of the intervention of type ι on the i-th variable, i.e., end device. The final outcome of risk assessment is given in Eq. (1) and is a vector of risk values for each attacked variable.

$$\Re_i = \sum_{\iota \in A} \omega_{i\iota} \cdot p_\iota, \forall i \in I, \tag{1}$$

where $p_\iota | \sum_{\iota \in A} p_\iota = 1$, is a vector containing the predefined probabilities for each type of cyber attack. Following, we provide the mathematical description for determining the severity matrix Ω. First, we compute the co-variance matrix $\Sigma^\iota, \forall \iota \in A$, as indicated in Eq. (2). Then, according to Eq. (3) we compute the factor loadings Z^ι by using the eigenvectors of Σ denoted by U. As stated in [14], the square of factor loadings represents "the proportion of the total unit variance of the indicator which is explained by the factor". Accordingly, Eq. (4) defines the variance ϑ_i^ι for each factor, where $v_i^\iota, \forall i \in I$ are the eigenvalues of Σ^ι. Next, using the above formulations, the severity matrix is defined by Eq. (5). For further convenient usage the severity matrix is normalized in the $[0, 1]$ interval. Finally, by *a priori* knowing the vector of probabilities p_ι, the application of Eq. (1) to determine the risk values $\Re_i$ for each attacked device becomes straightforward.

$$\Sigma^\iota = \frac{1}{n} C^\iota \cdot C^{\iota T}, \forall \iota \in A. \tag{2}$$

$$Z^\iota = U^{\iota T} \cdot C^{\iota T}, \forall \iota \in A. \tag{3}$$

$$\vartheta_i^\iota = \frac{v_i^\iota}{\sum_{l \in I} v_l^\iota}, \forall i \in I, \forall \iota \in A, \tag{4}$$

$$\omega_{i\iota} = \sum_{i \in I} Z_{il}^\iota \cdot \vartheta_l^\iota, \forall i, l \in I, \forall \iota \in A. \tag{5}$$

4 Optimal Control Network Design

In this section we employ the risk values to define a finite set of security levels. These serve as security level requirements for vulnerable variables, hereinafter referred to as end devices (ED). Then, a single linkage hierarchical clustering technique is applied to the risk values to develop a predefined number of ED groups. Each group corresponds to a security level requirement. As a constraint, an ED can connect to one of the concentrator nodes (CN) in order to maintain communication with supervisory and control stations. Therefore, the optimization problem discussed in this paper seeks the optimal connection of ED to CN by minimizing the overall distance between ED and CN, but taking into account the maximum link capacity of CN and the security level requirement of ED.

In the description of the optimization problem we use the following notations: we define $\mathcal{C} = \{1, 2, ..., \imath, ..., \mathfrak{c}\}$ to denote the set of concentrator nodes, $\mathcal{D} = \{1, 2, ..., \jmath, ..., \mathfrak{d}\}$ the set of end devices and $\mathcal{S} = \{1, 2, ..., \kappa, ..., \mathfrak{s}\}$ as the set of available/predefined security levels. Furthermore, the optimization problem needs to account for other network parameters, such as link capacity, traffic demands and security levels. Let $s^{\mathcal{C}}_{\imath\kappa}$ be a binary parameter to denote if the $\imath$-th CN supports the κ-th security level. Then, let $s^{\mathcal{D}}_{\jmath\kappa}$ be a binary parameter to denote if the risk assessment procedure has assigned the κ-th security level requirement to the $\jmath$-th ED. Next, we define a set of parameters to identify the geographical positioning of CN and of ED. In this respect the optimization problem uses two-dimensional coordinates involving $(x^{\mathcal{C}}_{\imath}, y^{\mathcal{C}}_{\imath})$ for CN and $(x^{\mathcal{D}}_{\jmath}, y^{\mathcal{D}}_{\jmath})$ for ED. Furthermore, since each CN has a limited processing capability, we define the link capacity parameter as $\zeta^{\mathcal{C}}_{\imath}$ and $\xi^{\mathcal{D}}_{\jmath}$ as the traffic demand of the connected ED. Depending on the values of $\xi^{\mathcal{D}}_{\jmath}$, the parameter $\zeta^{\mathcal{C}}_{\imath}$ indirectly defines the number of ED that can be connected to the $\imath$-th CN. Lastly, we define the variables for the connection of each ED to a CN. More precisely, we define the binary variable $\nu_{\imath\jmath}$ with value 1 if ED $\jmath$ connects to CN $\imath$. Essentially, the network design problem will identify the values for this variable such as to minimize the objective function. In practice, the objective of network design is to efficiently connect the ED to the CN, while taking into account the security requirements and the traffic demands. The overall installation cost and later on the operational costs depend on the distance between nodes and the required security levels. Furthermore, shorter distances can also reduce the communication delays. Therefore, the objective of the ILP problem is to minimize the Euclidean distances in such a way to connect each ED to the closest CN:

$$min\left(\sum_{\imath\in\mathcal{C}}\sum_{\jmath\in\mathcal{D}}\left[(x^{\mathcal{C}}_{\imath} - x^{\mathcal{D}}_{\jmath})^2 + (y^{\mathcal{C}}_{\imath} - y^{\mathcal{D}}_{\jmath})^2\right]\cdot\nu_{\imath\jmath}\right), \tag{6}$$

which is subject to the following constraints:

$$\sum_{\imath\in\mathcal{C}}\nu_{\imath\jmath} = 1, \forall\jmath\in\mathcal{D}, \tag{7}$$

$$s^{\mathcal{D}}_{\jmath\kappa}\cdot\nu_{\imath\jmath} \le s^{\mathcal{C}}_{\imath\kappa}, \forall\imath\in\mathcal{C}, \jmath\in\mathcal{D}, \kappa\in\mathcal{S}, \tag{8}$$

$$\sum_{\jmath\in\mathcal{D}}\xi^{\mathcal{D}}_{\jmath}\cdot\nu_{\imath\jmath} \le \zeta^{\mathcal{C}}_{\imath}, \forall\imath\in\mathcal{C}, \tag{9}$$

where Eq. (7) enforces that each ED is connected to a single CN. Constraint (8) enforces the connection of end devices to the concentrator nodes that support the required security level. Finally, constraint (9) ensures that the CN processing capacity is not exceeded.

5 Experimental Results

In this section we first apply the risk assessment technique to identify the risk levels of cyber assets. The risk levels are then applied in the evaluation of the network optimization problem, which is implemented and tested in AIMMS [1] by using the CPLEX solver. In the first instance we adopt the Tennessee Eastman chemical process (TEP) model [6]. Then, we validate the developed methodology by using the IEEE 14-bus electricity grid model enriched with control loops specific to real-world power systems, e.g., Power System Stabilizer (PSS), Automatic Voltage Regulators (AVR), Turbine Governors (TG), secondary voltage regulators including Cluster Controllers (CC), and Central Area Controllers (CAC). To demonstrate the scalability of the proposed techniques we perform the risk assessment and the network design on the IEEE 300-bus test system. The attack scenarios employed in the following experiments include bias injection and replay.

5.1 Results on the TEP

This case study considers four attack types and an attack probability defined by $p_\iota = [0.4, 0.3, 0.1, 0.2]$. In detail, the first attack type involves a 15% bias injection on control variables, with a duration interval of 0.1 h. In contrast, the second attack scenario injects a 60% bias value to each variable. The last two attack types are replay attacks, one with a duration of 4 h ($\epsilon = 4$ h) and the second on with a duration of $\epsilon = 3$ h. By knowing the probability values and the severity matrix resulted from the CAIA technique, we determine the final risk values for each investigated control variable or end device. For the case of the TEP, the risk values for devices are given in Fig. 1(a). Additionally, Fig. 1(b) presents the results of grouping the pure risk values using hierarchical clustering in 3 groups of security levels. Here, the usage of single linkage hierarchical clustering is needed to effectively categorize the end devices in a predefined number of security level groups. As the figure shows, the devices denoted by 1 and 8 have been assigned a higher security level, meaning that these devices require the most secure communication channels. In contrast, devices 4, 6, 7, 9, 10, 11 and 12

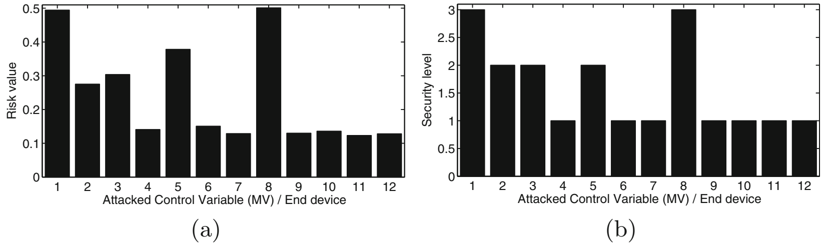
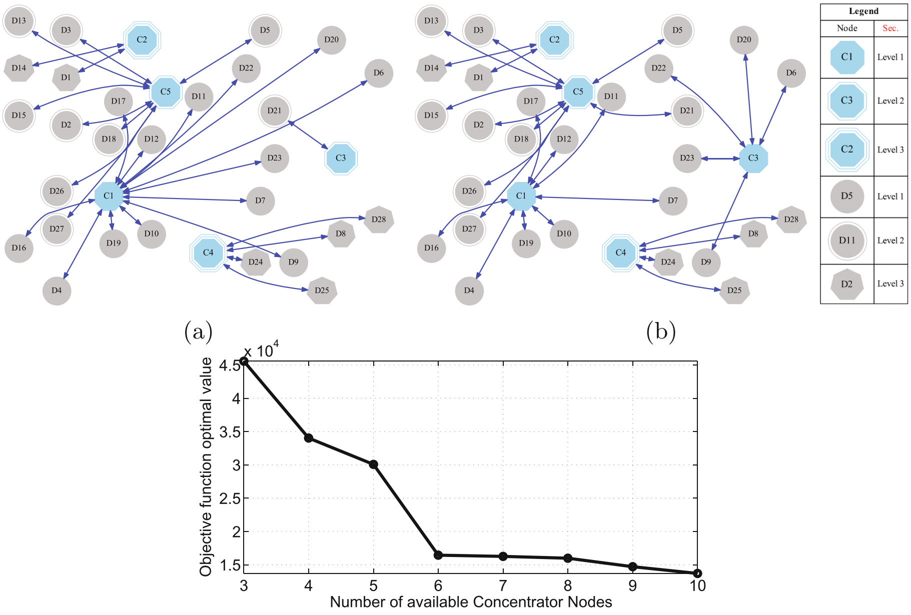


Fig. 1. Risk assessment outcome: (a) Pure risk values; and (b) Risk values enforced in 3 security level groups.

have been associated with low security level requirements, meaning that short-term cyber attacks performed on these devices won't critically affect the normal operation of TEP. Finally, in the network design phase the security requirement parameter of $s_{\jmath\kappa}^{\mathcal{D}}$ is initialized based on device groups, as depicted in Fig. 1(b).

In the following, we use the proposed network design approach in accordance with the above resulted risk values of the end devices. For network design experiments we assume five CN in five different locations of the plant. The end devices corresponding to control variables and the end devices corresponding to observed variables will connect to these five CN. However, in practice, CN are placed by considering the physical areas delimited by the experts or by the need of CN to cover the security and performance requirements of ED. Later on in this section multiple experiments with various CN are performed to identify the optimal number of CN in the case of the TEP. Let us first analyze the connection layout in Fig. 2(a). Security levels are illustrated with simple, double and triple symbol outlines in the case of CN, and simple outlined circle, double outlined circles and septagons in the case of ED, respectively. Furthermore, each node is placed as specified by the position parameters. As it is shown in Fig. 2(a) the overall connection distance is minimized in the presence of security and link capacity constraints. Subsequently, by refining the security level parameters of CN, and rerunning the network design framework, a different connection graph is



(a)

(b)

(c)

Fig. 2. Resulted network layout: (a) with initial parameters; (b) with C3's security level changed to 1 and (c) objective function's optimal values for different number of CN.

obtained in Fig. 2(b). The changing of C3's security level from 2 (mid-level) to a low level, radically changes the optimal connection layout as well. Therefore, the placement of CN heavily influences the network topology. This fact is illustrated through a series of experiments performed for different number of CN, while the rest of the parameters remained unchanged. Accordingly, the results shown in Fig. 2(c) express the final value of the objective function in contrast with the number of CN. Finally, we notice in Fig. 2(c) the steep decrease of the objective function's value, which indicates that 6 should be the optimal number of CN used for the network design (after 6 the cost function decreases slowly). In contrast with these results, practical situations may include additional restrictions in placing CN in some special areas, e.g., hazardous areas.

5.2 Results on the IEEE 14-Bus Electricity Grid

Making a step further, we show the application of the developed risk assessment technique on the 14-bus electricity grid model. Even though the grid comprises a slightly different architecture from that of the TEP's, the application of CAIA and of risk assessment remains mostly the same. First, we identify the assessed devices corresponding to each substation of the power grid. In this study it is considered that each substation is represented by a cyber device, which is part of the grid's SCADA network. Overall, four attack scenarios have been defined for the risk assessment. These are aimed to represent the main cyber security threats for the cyber realm. The first scenario implements cyber attacks that ultimately cause faults at substation levels. Assuming that proper load measurements and load control are key requirements in the stable operation of power grids, the second attack scenario induces load compensation disturbances. Considering the architecture of control loops, i.e., voltage controller modules localized at the substations including generator components, the third attack scenario launches integrity attacks against the IEC61850 protocol, which ensures the communication between AVR and other high level controllers, i.e., CC and CAC. Finally, the fourth attack scenario compromises remotely controlled line breaker devices to cause severe disruptions in the grid's structural stability. Figure 3 illustrates the changes in the output of risk assessment based on different attack scenarios and parameters. These results underline that different cyber attack vectors may yield different impact values and a different behavior of the physical process. Therefore, it is imperative that risk assessment to be conducted on multiple attack scenarios embracing a wide palette of parameters. Lastly, the final risk values for each end device are presented in Fig. 4(a). It is shown that substations 1, 2, 3 and 8 exhibit high risk values in the case of the four attack types. As a result, the hierarchical clustering approach (Fig. 4(c)) allocates to each available security level the appropriate device group. Since three security groups are expected, Fig. 4(b) illustrates the final security level of groups as an outcome of the risk assessment.

Lastly, we evaluate the developed methodology in the context of the IEEE 14-bus power grid. We assume a total of 14 ED, which need to be optimally connected to 5 CN. The results of the optimal security-aware configuration are

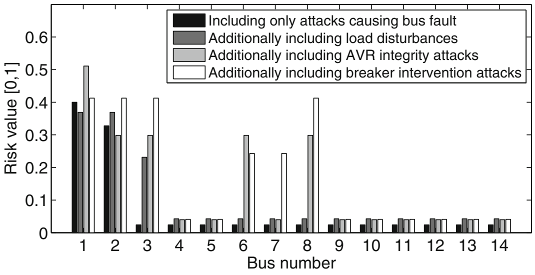
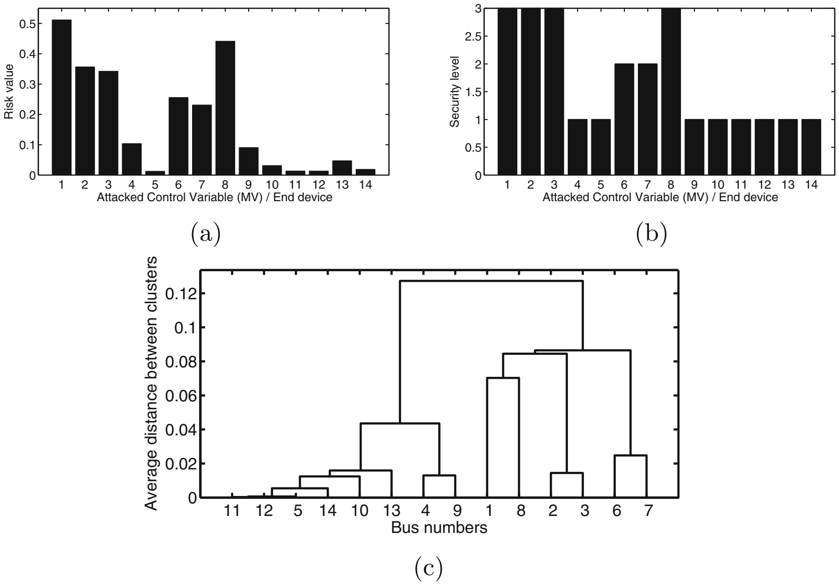


Fig. 3. Changes in risk assessment results by different attack scenarios.



(a)

(b)

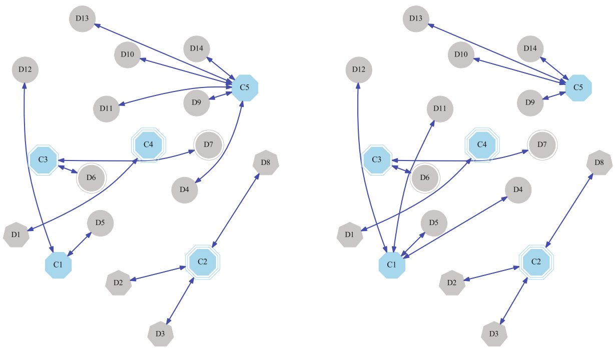
(c)

Fig. 4. Risk assessment outcome on the IEEE 14-bus grid model: (a) Pure risk values; (b) Risk values enforced in 3 groups with different security levels; and (c) Risk assessment dendrogram.

presented in Fig. 5(a). By changing the capacity of CN 5 in Fig. 5(b) we depict the changes in the output of the optimization problem.

5.3 Results on the IEEE 300-Bus Electricity Grid Model

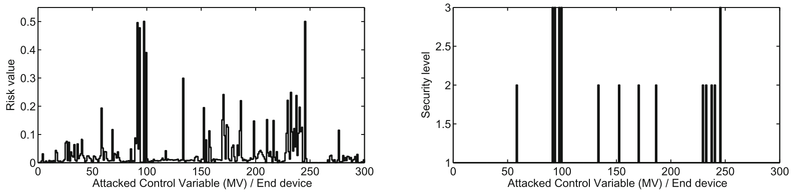
Finally, we show the scalability of the elaborated risk assessment procedure. The results in this section demonstrate its successful and representative application in the case of the large-scale IEEE 300-bus electricity grid model. To represent a wide variety of cyber attacks, the following experiments use two attack vectors, i.e., load disturbance attack and substation compromise. In the case of large-scale infrastructures we measure the isolation phenomenon, that is, attacks



(a) (b)

Fig. 5. Optimal network layout for the IEEE 14-bus electricity grid model: (a) unconstrained, and (b) constrained by the link capacity of C5.

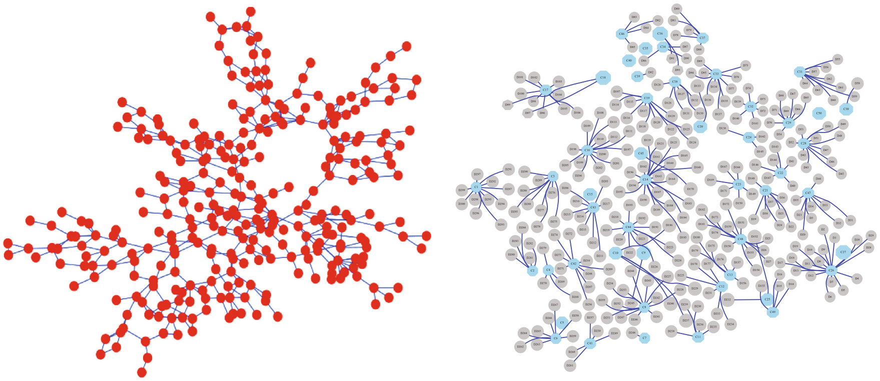
impacting a certain region of the grid. The calculated risk values are presented in Fig. 6, where we assume the same attack probability. However, depending on the expert's judgments the risk assessment can be changed to include different probabilities for each attack type. Figure 6(a) illustrates the peaks in risk values in the proximity of substations 100 and 250. This means that these devices have a greater impact on the overall operational stability of the grid. Accordingly, Fig. 6(b) groups the substations in three security level groups.



(a) (b)

Fig. 6. Risk assessment outcome on the IEEE 300-bus grid model: (a) Pure risk values; and (b) Risk values enforced in 3 security groups.

In accordance with the size of the model, the network design problem assumes the presence of 300 ED. In the first step the security levels of the CN are assigned proportionally according to the risk assessment results and the designated security requirements of ED (see Sect. 5.3). For illustration purposes we assume a scenario comprising of 50 CN. The connection diagram of Fig. 7(b) includes 36 low-level security CN, 10 mid-level security CN and 4 high-level security CN. Figure 7(a) represents the electrical topology, while Fig. 7(b) shows the final connection of ED to CN. The network layout accounts for the geographical distances



(a) (b)

Fig. 7. Optimal network layout for the IEEE 300-bus power grid model: (a) electrical topology [11], and (b) communication infrastructure with 50 CN.

between the nodes, but also embraces their security requirements, as delivered by the risk assessment methodology.

6 Conclusions

We developed a methodology for the optimal design of industrial networks. The approach embraces a risk assessment technique and an optimization problem to minimize connection distances, while enforcing security and capacity requirements. The experimental results revealed the importance of security-aware network design. As future work we intend to build a specialized software to assist engineers in designing optimal ICS networks.

Acknowledgment. This work was supported by a Marie Curie FP7 Integration Grant within the 7th European Union Framework Programme (Grant no. PCIG14-GA-2013-631128).

References

1. AIMMS: Advanced Interactive Multidimensional Modeling System (2015). http://www.aimms.com/aimms/. Accessed May 2016
2. Bilis, E., Kroger, W., Nan, C.: Performance of electric power systems under physical malicious attacks. IEEE Syst. J. **7**(4), 854–865 (2013)
3. Carro-Calvo, L., Salcedo-Sanz, S., Portilla-Figueras, J.A., Ortiz-Garca, E.: A genetic algorithm with switch-device encoding for optimal partition of switched industrial Ethernet networks. J. Netw. Comput. Appl. **33**(4), 375–382 (2010)
4. Chen, T., Abu-Nimeh, S.: Lessons from Stuxnet. Computer **44**(4), 91–93 (2011)
5. CrySiS Lab: sKyWIper (a.k.a. flame a.k.a. flamer): a complex malware for targeted attacks, May 2012

6. Downs, J.J., Vogel, E.F.: A plant-wide industrial process control problem. Comput. Chem. Eng. **17**(3), 245–255 (1993)
7. Ford, D.N.: A behavioral approach to feedback loop dominance analysis. Syst. Dyn. Rev. **15**(1), 3–36 (1999)
8. Genge, B., Haller, P., Kiss, I.: Cyber-security-aware network design of industrial control systems. IEEE Syst. J. **11**(3), 1373–1384 (2015)
9. Genge, B., Siaterlis, C.: Physical process resilience-aware network design for SCADA systems. Comput. Electr. Eng. **40**(1), 142–157 (2014)
10. Genge, B., Kiss, I., Haller, P.: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. IJCIP **10**, 3–17 (2015)
11. Hines, P., Blumsack, S., Cotilla Sanchez, E., Barrows, C.: The topological and electrical structure of power grids. In: 2010 43rd Hawaii International Conference on System Sciences (HICSS), pp. 1–10, January 2010
12. Kiss, I., Genge, B., Haller, P.: Behavior-based critical cyber asset identification in Process Control Systems under Cyber Attacks. In: 16th Carpathian Control Conference (ICCC), pp. 196–201, May 2015
13. Kundur, D., Feng, X., Liu, S., Zourntos, T., Butler-Purry, K.: Towards a framework for cyber attack impact analysis of the electric smart grid. In: First SmartGrid-Comm, pp. 244–249, October 2010
14. Nardo, M., Saisana, M., Saltelli, A., Tarantola, S., Hoffman, A., Giovannini, E.: Handbook on Constructing Composite Indicators. OECD Publishing, Paris (2005)
15. Sandberg, H., Amin, S., Johansson, K.: Cyberphysical security in networked control systems: an introduction to the issue. IEEE Control Syst. **35**(1), 20–23 (2015)
16. Sgouras, K., Birda, A., Labridis, D.: Cyber attack impact on critical smart grid infrastructures. In: 2014 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5, February 2014
17. Sridhar, S., Govindarasu, M.: Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid **5**(2), 580–591 (2014)
18. Symantec: Dragonfly: cyberespionage attacks against energy suppliers. Technical report (2014)
19. Zhang, L., Lampe, M., Wang, Z.: A hybrid genetic algorithm to optimize device allocation in industrial ethernet networks with real-time constraints. J. Zhejiang Univ. Sci. C **12**(12), 965–975 (2011)
20. Zhang, L., Lampe, M., Wang, Z.: Multi-objective topology design of industrial ethernet networks. Frequenz **66**(5–6), 159–165 (2012)