NETWORKED CRITICAL INFRASTRUCTURES: SECURE AND RESILIENT BY DESIGN

GENGE Béla, Associate Professor PhD,
„Petru Maior" University of Tîrgu Mureş

Abstract: *Networked Critical Infrastructures (NCI) such as electricity grids, oil and gas pipelines, ensure the smooth functioning of our society. Their protection from accidental failures or intentional attacks or sabotage is of paramount importance and a major societal challenge. In this work we briefly summarize our previous work on building novel methodologies that are aimed at designing secure, on the one hand, and resilient, on the other hand, NCI. We further identify possible opportunities to deliver a harmonized and complete security and resilience NCI design solution. Possible implementation solutions are presented including the provisioning of Software Defined Networks as the communication platform for NCI.*

Keywords: *networked critical infrastructures, security, resilience, integer linear programming.*

Introduction

Our modern society depends today on the smooth functioning of large scale infrastructures such as electricity grids, oil and gas pipelines, transportation systems, which due to their importance are often characterized as Networked Critical Infrastructures (NCI) – see Figure 1. Since these infrastructures deliver fundamental services to the economy and to the lives of all citizens their protection from accidental failures or intentional attacks or sabotage is of paramount importance and a major societal challenge which has been acknowledged not only by academia, industry but by policy makers as well [1, 2, 3]. Incidents such as the collapse of India's northern electricity in July 2012 [4] and more recently, cyber espionage attacks against energy suppliers [5] showed the true dimension of the risks that modern society faces from the increasing dependency on a growing number of infrastructures which are tightly interconnected, e.g., the energy grid was considered until recently independent but today its interdependency from Information & Communication Technologies (ICT) is widely recognized.

BDD-A23336 © 2015 Editura Universităţii „Petru Maior"
Provided by Diacronia.ro for IP 216.73.216.143 (2026-11-18 20:53:22 UTC)

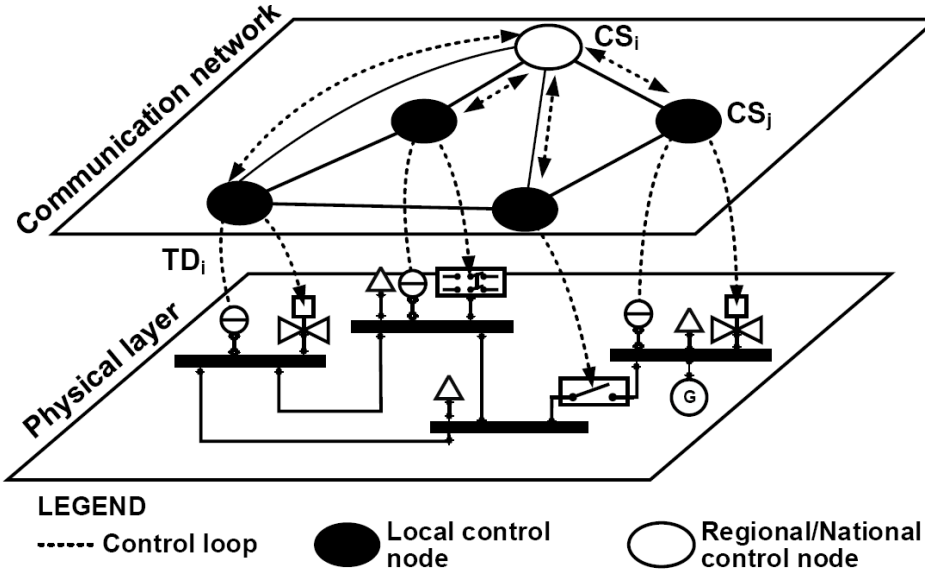


Figure 1: Architecture of modern Networked Critical Infrastructures.

All relevant actors have already shown the intention to contribute to the protection of NCI, i.e., researchers by proposing modern risk assessment methodologies, countermeasures or early warning systems, industry by revising security measures and operating guidelines [6] and policy makers through regulation enforcing a security baseline and incident monitoring. Nevertheless, these efforts are hindered by the lack of modern tools and a true understanding of the complexity of Critical Infrastructures, since current working tools, e.g., models, are stemming from an era which infrastructures were monolithic, mechanical and isolated. On top of these, the lack of tools to aid the design of secure and resilient CI, coupled with the large and critical number of NCI design requirements, leads to significant challenges in the identification of their architectural and communication features.

Therefore, in this work we argue that there is an acute need of methods and practical tools that integrate the wide range of NCI design requirements pertaining to quality of service, security, resilience, reliability, costs, geographical and hardware limitations, etc. Furthermore, we propose possible solutions coming from the field of mathematical optimizations and we show the possible application of such methodologies in the realistic design of NCI.

Critical Infrastructure Design Requirements

Specific guidelines for strengthening the security of the control systems embedded into NCI can be found in NIST's "Guide to Industrial Control Systems" [7]. From the network design point of view [7] recommends the

BDD-A23336 © 2015 Editura Universităţii „Petru Maior"
Provided by Diacronia.ro for IP 216.73.216.143 (2026-11-18 20:53:22 UTC)

segregation of networks into different zones in order to isolate and to better protect critical assets.
Similarly, one of the most significant references for CI network design is the ISA-62443.03.02 [8] series of standards. The first significant concept defined by ISA-62443.03.02 is the *security zone* denoting the "grouping of logical or physical assets that share common security requirements" [8]. Although this definition emphasizes "common security requirements", the ISA standard also recognizes the potential of grouping assets based on physical or logical location, operational function, required access, and responsible organization. An important consideration, however, is that the creation of security zones should be also subject to a high-level risk assessment which would deliver a relative risk ranking of cyber assets within a CI installation. This ranking facilitates the grouping of assets and the creation of specific security zones.
A second significant concept embraced by ISA-62443.03.02 are *conduits*, denoting "logical grouping of communication channels, between connecting two or more zones, that share common security requirements" [8]. Conduits ensure the proper ranking of communication lines between security zones and implement the necessary security measures for achieving the desired security properties.
Besides security measures, however, we should emphasize that NCI are subject to a set of Quality of Service (QoS) considerations pertaining to specific characteristics of industrial installations. Amongst others, we mention strong determinism, real-time data transfer, hierarchical architecture, and small packets of periodic traffic. Additional QoS parameters have been summarized in references [9] and [10].
Lastly, resilience and fault tolerance in industrial installations is usually achieved through the allocation of separate (secondary) back-up communication lines, physically separated from the primary communications network [11, 12]. Primary and secondary communications have different QoS values and are implemented with a variety of techniques ranging from military-grade broadband switches, Asynchronous Transfer Mode (ATM) networks, Power Line Carriers (PLC), to modern communication infrastructures such as Multi Protocol Label Switching (MPLS).
As it can be seen from the above-mentioned discussion, NCI design is not a trivial problem. Furthermore, besides these, there can be various other requirements addressing the cyber and the physical dimensions of NCI.

Designing Secure Networked Critical Infrastructures

While the traditional industrial network design problem is a well-known field of research [13, 14, 15], the security and resilience design has only been

BDD-A23336 © 2015 Editura Universităţii „Petru Maior"
Provided by Diacronia.ro for IP 216.73.216.143 (2026-11-18 20:53:22 UTC)

recently addressed. Our previous work [16] expands the traditional NCI network design problem with security requirements aimed at constructing solutions to the design of modern infrastructures. The approach encompasses design criteria intended to fulfill typical NCI communication requirements, e.g., high-speed messages must be delivered in the 2ms to 10ms range, economical constraints, and security recommendations outlined by International Society of Automation (ISA) in ISA-62443.03.02 (July 2014).
The developed mathematical foundation of the secure NCI network design problem was built on the traditional network design problem as formulated by Capone *et al.* in [15]. However, the work presented in [15] was adapted and expanded in order to accommodate specific characteristics of ICS networks and ICS communications, and to integrate ICS security recommendations outlined in ISA-62443.03.02. More specifically, given the deterministic nature of NCI traffic, the problem formulated in [15] was reformulated by ensuring that individual demands are unsplittable (non-bifurcated) and are routed on well-known communication paths established at design-time. Furthermore, the network design problem was expanded to accommodate specific characteristics of underlying physical processes, and of metrics of cyber attack impact and process observability. We also incorporated security recommendations pertaining to security zones and conduits as outlined in the ISA-62443.03.02 standard. Finally, we expanded the network design problem with communication QoS requirements to ensure real-time constraints are met for each individual demand.
Based on these aspects, the cyber security NCI network design problem can then be viewed as an objective problem that minimizes the costs of the installation and ensures that a wide variety of constraints are satisfied. In [16], the mathematical model of NCI design problem was formulated as an integer linear programming (ILP) problem.

Designing Resilient Networked Critical Infrastructures

Besides cyber security requirements, however, a major design requirement is the resilience of the communication infrastructure. In this case we assume that traffic demands are routed across a meshed topology consisting of data concentrator nodes. These are well-known elements in the architecture of smart energy networks, and are mainly destined to aggregate and forward data from/into various communication mediums. Data concentrators may be implemented in various locations to aggregate data from several Home/Neighborhood Area Networks, substations, and to ensure that data is available to the utility and to customers.

BDD-A23336 © 2015 Editura Universităţii „Petru Maior”
Provided by Diacronia.ro for IP 216.73.216.143 (2026-11-18 20:53:22 UTC)

Similarly to the approach described earlier in this paper, in our previous work [17] we have adopted a mathematical model of the NCI design as an Integer Linear Programming (ILP) problem. In the developed ILP problem traffic demand paths, end-points, and concentrator sites are installed in such a way to minimize the costs of the infrastructure, while ensuring that constraints regarding real-time packet delivery, reliability, and resilience are satisfied.

Designing Secure and Resilient Networked Critical Infrastructures

The above two approaches provided separate solutions to the cyber security and resilience design of NCI. However, it can be intuitively conceived that since both design problems represent Integer Linear Programming models, their building blocks may be easily combined into one problem. This intuition is further supported by the fact that in both cases the objective function minimizes network design costs. Their combination may thus lead to a comprehensive and integrated design methodology for NCI.

To start with, the optimization problem of the secure and resilient design methodology will minimize costs. Then, the constraints of each problem may be adopted and harmonized in order to create a complete ILP problem.

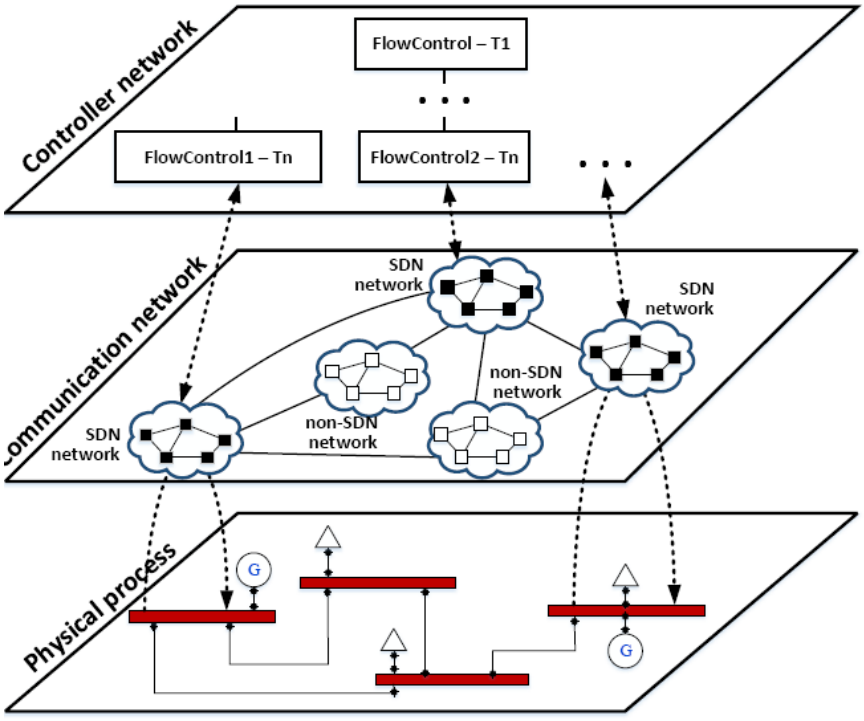


Figure 2: Software Defined Networking architecture for secure and resilient NCI.

BDD-A23336 © 2015 Editura Universităţii „Petru Maior”
Provided by Diacronia.ro for IP 216.73.216.143 (2026-11-18 20:53:22 UTC)

While the ILP problem may identify the necessary communication infrastructure, its actual implementation highly depends on the designers and on the available technology. However, nowadays, industrial operators are adopting advanced networking solutions from the field of traditional IP networking in order to increase the security and resilience of communication infrastructures. Solutions including Multi Protocol Label Switching (MPLS) and Software Defined Networking (SDN) have recently been adopted to replace older implementations based on Frame Relay and Asynchronous Transfer Mode (ATM). Nevertheless, communications in large-scale NCI usually cross the boundaries of one organization. Therefore, the communication infrastructure may comprise several networks including SDN-enabled communications alongside non-SDN networks.

Therefore, in such an SDN platform we need to account for a heterogeneous communication architecture where SDN-enabled networks are provisioned together with non-SDN networks. An overview of such a possible communication platform is presented in Figure 2. Here, we distinguish between three separate dimensions of SEN. The physical dimension comprises the underlying physical process, that is, the energy network including generators, loads, substations, and power lines. On the other hand, the communication network comprises the SDN switches, the communication lines between SDN switches and the non-SDN networks. Finally, the controller dimension encapsulates several flow controllers. These are organized in an n-Tier hierarchical structure, where each tier includes several flow controllers.

The adoption of SDN-based solutions in delivering a secure and resilient NCI needs to account, however, on the fact that SDN communication lines do not encapsulate security measure. It is therefore up to the designer to identify and to adopt the appropriate security measures.

Conclusions

In this work we briefly discussed the opportunities for building innovative tools that embrace the cyber security and the resilience requirements for designing modern NCI. Such an approach could be built on a classic optimization problem such as Integer Linear Programming, in which the objective may minimize the installation's costs, while the constraints can impose the satisfaction of various constraints. Nevertheless, besides such design problem formulations we have also identified a possible implementation solution. Such a solution can come from the field of traditional IP networking where Software Defined Networks have already been proven to be a candidate for delivering resilient communication infrastructures. Nevertheless, a significant effort is still needed in order to secure the

BDD-A23336 © 2015 Editura Universităţii „Petru Maior”
Provided by Diacronia.ro for IP 216.73.216.143 (2026-11-18 20:53:22 UTC)

communication lines of Software Defined Networks, and to ensure the harmonization of design-time and of installation-specific information and of the available technologies.

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] Commission of the European communities, "Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786", 2006.
[2] Commission of the European communities, "Communication from the Commission: A Digital Agenda for Europe, COM(2010) 245", 2010.
[3] Reuters, Obama turns focus to Internet security, privacy, http://www.reuters.com/article/2015/01/10/us-usa-obama-cybersecurity-idUSKBN0KJ0KF20150110.
[4] Amol Sharma, Saurabh Chaturvedi, and Santanu Chaudhury, "India's Power Network Breaks Down", The Wall Street Journal, July 31, 2012.
[5] Symantec, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers", Technical Report, 2014.
[6] Unisys Survey Reveals Nearly 70 Percent of Critical Infrastructure Providers Have Been Breached in the Past Year, 2014, http://www.unisys.com/offerings/security-solutions/News%20Release/Unisys-Survey-Reveals-Critical-Infrastructure-Providers-Breached
[7] K. S. K. Stouffer, J. Falco, "Nist sp 800-82 guide to industrial control systems (ICS) security. revision 1," National Institute of Standards and Technology, 2013.
[8] International Society of Automation, "IEEE Security for Industrial Automation and Control Systems: Security Risk Assessment and System Design (ISA-62443.03.02 (99.03.02)," 2014.
[9] B. Galloway and G. Hancke, "Introduction to industrial control networks," Communications Surveys Tutorials, IEEE, vol. 15, pp. 860–880, Second 2013.
[10] J.-P. Thomesse, "Fieldbus technology in industrial automation," Proceedings
of the IEEE, vol. 93, pp. 1073–1101, June 2005.
[11] A. Bobbio, G. Bonanni, E. Ciancamerla, R. Clemente, A. Iacomini, M. Minichino, A. Scarlatti, R. Terruggia, and E. Zendri, "Unavailability of critical scada communication links interconnecting a power grid and a telco network," Reliability Engineering & System Safety, vol. 95, no. 12, pp. 1345–1357, 2010.

BDD-A23336 © 2015 Editura Universităţii „Petru Maior"
Provided by Diacronia.ro for IP 216.73.216.143 (2026-11-18 20:53:22 UTC)

[12] IBM and Cisco, "Cisco and IBM provide high-voltage grid operator with increased reliability and manageability of its telecommunication infrastructure," IBM Case Studies, 2007.
[13] G. Nan, Z. Mao, M. Yu, M. Li, H. Wang, and Y. Zhang, "Stackelberg game for bandwidth allocation in cloud-based wireless live-streaming social networks," Systems Journal, IEEE, vol. 8, pp. 256–267, March 2014.
[14] E. Amaldi, A. Capone, S. Coniglio, and L. Gianoli, "Network optimization problems subject to max-min fair flow allocation," Communications Letters, IEEE, vol. 17, pp. 1463–1466, July 2013.
[15] A. Capone, J. Elias, and F. Martignon, "Models and algorithms for the design of service overlay networks," Network and Service Management, IEEE Transactions on, vol. 5, pp. 143–156, September 2008.
[16] B. Genge, P. Haller, I. Kiss, "Cyber Security-Aware Network Design of Industrial Control Systems," IEEE Systems Journal, IEEE Systems Council, 2015.
[17] B. Genge, P. Haller, I. Kiss, "A Linear Programming Approach for K-Resilient and Reliability-Aware Design of Large-Scale Industrial Networks," International Conference on Ad Hoc, Mobile, and Wireless Networks (ADHOC-NOW), Lecture Notes in Computer Science, Volume 9143, Athens, Greece, pp. 288-302, 2015.

BDD-A23336 © 2015 Editura Universităţii „Petru Maior"
Provided by Diacronia.ro for IP 216.73.216.143 (2026-11-18 20:53:22 UTC)