Rafał Kozik

Michał Choraś

Institute of Computer Science and Telecommunications, UTP University of Science and Technology, Bydgoszcz, Poland

Witold Hołubowicz

Rafał Renk
Adam Mickiewicz University, Poznań, Poland
Institute of Computer Science and Telecommunications, UTP University of Science and Technology, Bydgoszcz, Poland

Increasing Protection and Resilience of Critical Infrastructures – Current challenges and approaches

Keywords

Critical Infrastructure Protection, simulation, security, cyber security, Next Generation Infrastructures (NGI)

Abstract

In this paper we present current key challenges with respect to Critical Infrastructure Protection and to their resiliency. As our world becomes more and more interconnected via open networks with the cyberspace, many new challenges arise. Therefore, we frame the problem within three distinctive domains: real world natural events, human (organisational and legal), and cyber one. Within our analysis we present how current technologies, tools and methodologies can be used to address certain problems within those domains. Moreover, we stress the fact that there is a limited number of initiatives that aim at proposing the holistic (all hazard) approach addressing all the domains at once.

1. Introduction

Nowadays, there is a significant effort focused on national Critical Infrastructure (CI) evaluation, simulations and threats analysis. It is caused by the fact that societies become more and more dependent on Critical Infrastructure. When one of these is malfunctioning we can significantly suffer from economic or societal damage. Moreover, serious damages of Critical Infrastructure may even lead to loss of human life.

Another challenging factor is the fact that many European Critical Infrastructures are becoming more and more dependent on one another, forming a complex system of systems. As the complexity is increasing, new potential threats are emerging, too. Moreover, due to the climate changes, CI are becoming more vulnerable to catastrophic meteorological events.

What is more, current state of the art shows that beside natural disasters and events the cyber-related threats are more and more dangerous. Therefore, there is an increasing number of initiatives, approaches, and tools that incorporate those aspects into strategic analysis of infrastructure disruptions, consequences evaluation, and assessment of systems dependencies.

Therefore, it is important that Critical Infrastructure stakeholders (operators, civil protection authorities, etc.) are equipped with tools that allow them to comprehend the complex nature of interconnected CI in order to identify possible threats, predict events, and be better prepared for crisis mitigation.

Despite the fact that recently much research related to CI protection and resilience has been conducted in Europe, the practical adoption of its results is below the expectations. For instance, Europe is still missing the institution similar to US NISAC (National Infrastructure Simulation and Analysis Center). NISAC provides CI operators, civil protection

agencies and other stakeholders with advanced capabilities increasing national preparedness.
The European project CIPRNet responds to many challenges related to CI protection and one of its major long-lasting goals is to establish EISAC (European Infrastructure Simulation and Analysis Center). Some findings and developments of CIPRNet are overviewed in Section 3, which is preceded by the presentation of current challenges and threats to Critical Infrastructure in Section 2. Conclusions are given thereafter.

2. Current challenges

In this section we analyse different challenges to Critical Infrastructure protection and resilience. As it is shown in Fig.1, the origin of these challenges can be roughly identified as related to three aspects: (i) Cyber (cyber threats and attacks, cyber terrorism, cybercrime), (ii) Natural World (climate events, earthquakes, etc.), and (iii) Human, Organisational and Legal one (law, roadmaps, human factors, etc.).

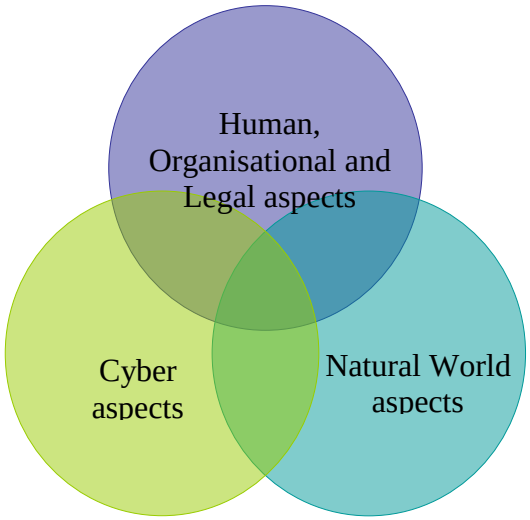

Figure 1. Origins of the current challenges in CI protection and resilience

2.1. Natural Disasters

Recently, due to the climate change, the number of meteorological events that impact the CI has significantly increased. These events typically include such disasters as: flooding, landslides (common result of flooding), hurricanes, drought, etc.
However, geological events, like earthquakes, volcanos eruptions, etc., are also occurring quite often. Challenging here is also the fact that events like earthquakes are practically impossible to predict.
One of the examples showing the impact of natural disasters on Critical Infrastructure is flooding that occurred in Middle-East Europe in 2002. In [11] it was explicitly emphasised that the lack of simulation tools allowing the local government to predict the behaviour of Elbe and Danube rivers caused significant impact on communication systems, hospitals, and transportation. It further resulted in poor coordination and low effectiveness of deployed mitigation and recovery plans.
Another example of the past natural disaster showing how so called cascading effects can cause significant damages is an earthquake that hit Kobe (Japan) area in 1995 [20]. Due to this catastrophic event the majority of transportation infrastructure was destroyed. This significantly impacted rescue actions and access to hospitals and paralysed that area.
Therefore, it is important to all CI stakeholders (CI operators, civil protection, etc.) to have tools that will allow them to understand the complex relation and dependencies between different Critical Infrastructures. Moreover, these tools should also improve CI stakeholders preparedness and effectiveness during response to crisis.

2.2. Cyber Security aspects

Industrial Control Systems (ICS) are ICT (Information and Communication Technology) solutions and their main role is to support industrial and critical processes. These systems are responsible for monitoring and controlling of a variety of aspects concerning Critical Infrastructure, such as water and waste control, energy, oil and gas refining and transportation. Recently the ICS have been transformed to systems that are highly interconnected with corporate networks and the Internet. Therefore, they became the inherent elements of the cyber ecosystem with new challenging problems caused by cyber threats and cybercrime.
Moreover, legacy systems have evolved from dedicated solutions for a particular operator to integrated and IP-based frameworks. This evolution has exposed the Critical Infrastructure to threats coming from the cyber domain.
As a result, in many cases a new approach to Critical Infrastructure protection is required. This approach should engage expert knowledge, decision support systems and such network elements as firewalls, intrusion and anomaly detection systems. That was not the case when the systems controlling Critical Infrastructure were designed and deployed.
Therefore, currently there is a significant research effort focusing on novel techniques (e.g. data mining and machine learning [6]) dedicated to cyber attacks detection. Moreover, as wireless sensors (WSN) technology is recently gaining in popularity and frequently used to monitor different aspects of

Critical Infrastructure, also an increasing number of research activities is concerning the methods for hardening this technology against cyber attacks [5], vulnerabilities identification and analysis [3], and secure data exchange [4].

It is also worth noticing that the way the cyber security has been perceived by the international community changed, when a massive cyber attack targeting Estonia made the whole national infrastructure stand still in 2007. At the peak of the crisis, the Internet, banks and mobile phone networks became unavailable.

What is more, dedicated systems controlling industrial processes (e.g. ICS systems) have also been facing an increased amount of cyber security incidents, such as Stuxnet worm. In result, in many countries, national entities and research institutions started to pay attention to cyber security. It resulted in a better understanding of the fact that many industry sectors strongly rely on ICT infrastructures and electronic communication channels.

Moreover, to provide interoperability, plenty of Industrial Control Systems use commonly available ICT infrastructures. What is more, the number of ICS adapting popular operating systems like Windows and Linux is also increasing. This fact is commonly used by cyber criminals to exploit vulnerabilities of operating systems in order to get access to sensitive data and network assets.

2.3. Human, Organisational and Legal aspects

As the interconnectivity of different Critical Infrastructures with ICT systems is constantly increasing, it is necessary to understand the underpinnings of the cyber ecosystem in order to better identify threats related to that domain.

The cyber ecosystem foundation is a legal framework that regulates cyber-related matters. Upon that foundation a Security Strategy is developed. Currently, the majority of European countries have established their national security strategies (NCSS). Such national strategies commonly refer to aspects like internal security, foreign and defence policy, as well as economy. Recently, the cyber dimension has also been addressed and included into the majority of national security strategies all over the world [13].

According to the EU ENISA overview document, NCSS as a strategic document usually defines the common general actions contributing to the cyber security domain, e.g.:"... to reduce the risk and secure the benefits of a trusted digital environment for businesses and individuals..." [24].

It also defines the main objectives. Some examples extracted from the UK NCSS [24] are: (i) "to tackle cybercrime", (ii) "to be more resilient to cyberattacks", (iii) "to have the cross-cutting knowledge, skills and capability [...] to underpin [...] security objectives".

As noticed by authors in [13], a national strategy does not define explicit methods to achieve the stated goals. However, it has significant influence on government, policy-makers and all other national and European bodies that have all necessary resources to deploy such strategy. An overview and comparison of different cyber security strategies is presented by Luiijf et al. in [15].

There is also the cyber security strategy prepared at the European level [8]. It is focused on such aspects as: (i) capabilities and response networks, for sharing information with public and private sector, (ii) governance structure, (iii) incident reporting for critical sectors like energy, water, finance and transport, (iv) global cooperation, to address global interdependencies and the global supply chain.

Apart from strategy development and implementation, the need for such organisational aspects like training should also be emphasised. Only knowledgeable and well-trained staff can implement the strategies and operate complex and interconnected Critical Infrastructures for the well-being of societies. Often, the lack of training and the lack of awareness are mentioned as the important threat for CI.

3. Increasing Protection and Resilience – different methods and approaches

3.1. Tools predicting natural events

Currently one of the initiatives that plan to make a step toward establishing the European equivalent of NISAC simulation centre is the FP7 CIPRNet project [9]. The project aims at creating new capabilities for CI operators and emergency managers. One of its objectives is also to integrate the research bodies scattered across Europe into so-called Virtual Centre of Competences (VCC). CIPRNet also performs research and development activities. So-called CIPRNet services include: simulation-based threat forecasting, natural events sensing and visualisation, threat visualisation, what-if and consequence analysis. The goal of such services development is to increase the situational awareness of the decision makers by extraction of the most necessary information from the large amount of heterogeneous data coming from different sources (such as real-time sensorial data).

Projects like CIPRNet are focusing on predicting possible natural events, identifying threats and assessing their impact on Critical Infrastructure. For the CI stakeholders it is important to have adequate

and accurate models and tools that allow them to address the CI protection and resiliency challenges.
However, in order to have a good and big operational picture of these aspects, it is also important to incorporate cyber domain into analysis processes.

3.2. Reactive and proactive approach in cyber domain

One of the projects that deal with the aspects related to cyber domain is CockpitCI project [10]. The project aims to improve the resilience and dependability of Critical Infrastructure by the automatic detection of cyber-threats and the sharing of real-time information about attacks among CI owners.
Another example is the finalised INSPIRE [2] project, that (beside real-time cyber-threats detection) tried to model with semantic language (so-called ontology) interdependencies between the Industrial Control System and the cyber security aspects. On that data model decision support system is provided (called INSPIRE Decision Aid Tool – DAT) with all the necessary information about the threats and vulnerabilities the specific Critical Infrastructure is exposed to. Additionally, DAT can propose appropriate reactions and countermeasures for the particular threat.

3.3. Decision support

Decision Support Systems (DSS) are information systems that support human in different decision-making activities. The DSS applications are successfully and widely used in industry and Critical Infrastructure protection (CIP).
The DSS systems are successfully used to manage river systems (e.g. to cope with floods). For instance, the German Federal Institute of Hydrology (BfG) is using such kind of DSS to manage the Elbe river system. Its importance was demonstrated during the grate flooding in 2002.
The DSS are also successfully deployed in the energy sector [25] nuclear power plants [14], urban water pollution control [27] or oilfield flood precaution [26].
All above-mentioned examples of DSS systems are focused on some particular aspects of Critical Infrastructure. However, designing an adequate and efficient DSS system is a difficult and challenging task.
Also FP7 CIPRNet and RoMA [21] projects plan to provide advanced DSS for Critical Infrastructure protection and for crisis management. Those prototypes would provide novel capabilities such as forecasting and consequence analysis.

3.4. Strategic-based approaches as a tool increasing resiliency

It must be noticed that reacting to current events which may occur both in real world and in cyber domain, as well as predicting capabilities and ability to assess the impact of such events on Critical Infrastructure are crucial to address the resilience and CI protection aspects. However, both security and resilience are not products that can be purchased by operator and simply deployed in the field.
As a matter of the fact, ICS are designed to be reliable in terms of confidentiality and availability, but security policies and practices are often not well implemented. In many cases, ensuring security and resilience are long-lasting and iterative processes that have to be coordinated.
Therefore, we believe that activities taking place on a strategic level are of the same importance as before-mentioned decision support systems, CI models and simulators, and cyber security solutions.
During this research we have analysed several general-purpose and sectoral roadmaps [1], [7], [11], [12], [17]-[19], [22]-[23]. The general-purpose roadmaps are focused on a wide spectrum of challenges and define various milestones, often at a different level of abstraction.
There are several common points of their agendas that could be considered as the high priority challenges, such as: (i) evaluation of system security, (ii) identity management mechanisms, (iii) improvements of analytical tools for security monitoring, (iv) response and recovery efforts, and (v) situational understanding.
The sectoral roadmaps are focused on industrial ICT infrastructures used in various domains (e.g. energy delivery, transportation). The main objectives defined in these roadmaps are similar to these defined in the general-purpose roadmaps, since the industrial infrastructures are a part of the whole ecosystem.
Therefore, the key points presented in the analysed roadmaps are also similar and they are the following: (i) evaluation of system security, (ii) insufficient focus on ICS modelling and simulation, (iii) protective techniques and technologies, (iv) culture of cyber security, knowledge and information sharing.

4. Conclusion

In this paper, different aspects related to the CIP community and decision makers are presented in the context of decision (support) making process. We have framed the problem within three distinctive domains related to natural events, human (organisational and legal) aspects, and cyber aspects.

Within our analysis we have identified different approaches that aim at addressing the problems related to each of the domains.

As it was presented in the paper, the problem of Critical Infrastructure dependencies, which among others stems from an increasing interconnectivity of different Industrial Control Systems via open network, causes different challenges in the context of Critical Infrastructure Protection.

Moreover, it can be noticed that the European Union is still lacking the simulation centres. What is more, in many cases security policies and practices are not well implemented, as well as legal regulations do not always follow the current state of technology. Therefore, in this paper we stressed the fact that also activities at the strategic level can be perceived as effective tools eventually increasing the security and resiliency of Critical Infrastructure.

Acknowledgements

The CIPRNet project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450. The European Commission's support is gratefully acknowledged.

The work is also funded by the Polish National Centre for Research and Development (NCBiR) from funds for science in the years 2013-2016, allocated for the international projects.

References

[1] Berenson, J. et al. (2012). *The Roadmap to Secure Control System in the Transportation Sector.* The Roadmap to Secure Control Systems in the Transportation Sector Working Group.

[2] Choraś M., Flizikowski A., Kozik R., Renk R. & Hołubowicz W. (2009). Ontology-Based Reasoning Combined with Inference Engine for SCADA-ICT Interdependencies, Vulnerabilities and Threats Analysis. *In Pre-Proc. of 4th International Workshop on Critical Information Infrastructures Security,* CRITIS'09, Bonn, Germany, 203-214, Fraunhofer IAIS.

[3] Coppolino, L., D'antonio, S. & Romano, L. (2014). Exposing vulnerabilities in electric power grids: An experimental approach. *International Journal of Critical Infrastructure Protection*, Vol. 7, issue 1, 51-60.

[4] Coppolino, L., D'Antonio, S., Elia, I.A. & Romano, L. (2011). Security Analysis of Smart Grid Data Collection Technologies. *Computer Safety, Reliability, and Security Lecture Notes in Computer Science* Vol. 6894, 143-156

[5] Coppolino, L., D'Antonio, S., Formicola, V. & Romano, L. (2013). Enhancing SIEM technology to protect critical infrastructures. *Critical Information Infrastructures Security Lecture Notes in Computer Science* Vol. 7722, 10-21.

[6] Coppolino, L., D'Antonio, S., Garofalo, A. & Romano, L. (2013). *Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks.* P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on.

[7] Eisenhauer, J., Donnelly, P., Ellis, M. & O'Brien, M. (2006). *Roadmap to Secure Control Systems in the Energy Sector.* U.S. Department of Energy, U.S. Department of Homeland Security.

[8] EU cyber security strategy (2013). http://www.enisa.europa.eu/media/newsitems/new-eu-cybersecurity-strategy-directive-announced

[9] FP7 CIPRNet project homepage https://www.ciprnet.eu

[10] FP7 CockpitCI project homepage http://www.cockpitci.eu/

[11] Jereza, K. et al. (2011). *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. ESCSWG (Energy Sector Control Systems Working Group).

[12] Johnson, S., Larson, B., Edwards, D. & Morley, K. (2008). *Roadmap to Secure Control Systems in the Water Sector.* Water Sector Coordinating Council Cyber Security Working Group (WSCCCWG).

[13] Klimburg, A. (Ed.) (2012). *National cyber security framework manual.* NATO Cooperative Cyber Defense Center of Excellence.

[14] Lee, S.J., Mo, M. & Seong, P.H. (2007). Development of an Integrated Decision Support System to Aid the Cognitive Activities of Operators in Main Control Rooms of Nuclear Power Plants. *Proc. of IEEE Symposium on Computational Intelligence in Multicriteria Decision Making* (MCDM), 146 152.

[15] Luiijf, E., Besseling, K. & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures,* Vol. 9 No. 1/2.

[16] Luiijf, E.A.M. & Klaver, M. H A (2005). Critical infrastructure awareness required by civil emergency planning. *Critical Infrastructure Protection, First IEEE International Workshop on.*

[17] Markatos, E. & Balzarotti, D. (2013). *The Red Book: A Roadmap for Systems Security Research*. SysSec (FP7 NoE Project).

[18] NIST (National Institute of Standards and Technology) (2014). *NIST Roadmap for Improving Critical Infrastructure Cybersecurity.*

[19] Pederson, P., Roxey, T. & Gray, J. (2011). *Cross-sector Roadmap for Cybersecurity of Control Systems*. ICSJWG (Industrial Control Systems Joint Working Group).
[20] Risk Management Solutions, Inc. (2005). *1995 Kobe Earthquake 10-year Retrospective*. Newark, CA.
[21] RoMA project - Resilience Enhancement of Metropolitan Areas. http://www.cis.uniroma1.it/en/node/5619
[22] U.S. Department of Homeland Security (2009). *A Roadmap for Cybersecurity Research*.
[23] U.S. Department of Homeland Security (2010). *Dams Sector Roadmap to Secure Control Systems*.
[24] UK Cabinet Office (2011). *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*.
[25] XiaoFeng, D., YuJiong, G. & Kun, Y. (2008). Study on Intelligent Maintenance Decision Support System Using for Power Plant Equipment. *Proc. of the IEEE International Conference on Automation and Logistics* Qingdao, China, 96100.
[26] Xie, L., Wang, Z. & Bian, L. (2008). The Research of Oiled Flood Precaution Decision Support System. *Proc. of International Seminar on Business and Information Management*, ISBIM '08, vol.2, 236 239.
[27] Zhang B., Wu G. & Shang S. (2008). Research on Decision Support System of Water Pollution Control Based on Immune Agent. *Proc. of International Symposium on Computer Science and Computational Technology, ISCSCT*, vol.1, 114117.