White Paper on Industry Experiences in Critical Information Infrastructure Security: A Special Session at CRITIS 2019

Giacomo Assenza[1], Valerio Cozzani[2], Francesco Flammini[3], Nadezhda Gotcheva[4], Tommy Gustafsson[5], Anders Hansson[6], Jouko Heikkila[4], Matteo Iaiani[2], Sokratis Katsikas[9], Minna Nissilä[4], Gabriele Oliva[1], Eleni Richter[7], Maaike Roelofs[8], Mehdi Saman Azari[3], Roberto Setola[1], Wouter Stejin[8], Alessandro Tugnoli[2], Dolf Vanderbeek[8], Lars Westerdahl[5], Marja Ylönen[4], and Heather Young[8]

[1] University Campus Biomedico of Rome, Italy
[2] University of Bologna, Italy
[3] Linnaeus University, Sweden
[4] VTT Technical Research Centre of Finland, Finland
[5] Swedish Defence Research Agency, Linköping, Sweden
[6] Sectra Communications AB, Teknikringen 20, 58330 Linköping, Sweden
[7] EnBW Energie Baden-Württemberg AG, Durlacher Allee 93, 76131 Karlsruhe, Germany
[8] TNO, Netherlands Organisation for Applied Scientific Research, Netherlands
[9] Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. The security of critical infrastructures is of a paramount importance nowadays due to the growing complexity of components and applications. This paper collects the contributions to the industry dissemination session within the 14th International Conference on Critical Information Infrastructures Security (CRITIS 2019). As such, it provides an overview of recent practical experience reports in the field of critical infrastructure protection (CIP), involving major industry players. The set of cases reported in this paper includes the usage of serious gaming for training infrastructure operators, integrated safety and security management in the chemical/process industry, risks related to the cyber-economy for energy suppliers, smart troubleshooting in the Internet of Things (IoT), as well as intrusion detection in power distribution Supervisory Control And Data Acquisition (SCADA). The session has been organized to stimulate an open scientific discussion about industry challenges, open issues and future opportunities in CIP research.

1 Introduction

Critical infrastructures must fulfil dependability requirements that impose the use of rigorous techniques during procurement, development, commissioning and training/preparedness, as well as in regulatory audits of the operational systems.

In this CRITIS special session we have solicited short presentations from an industrial perspective addressing any aspect of such processes and of the supervision of critical operations. Reports of actual cases were welcome including success stories or failure/emergency management operations with the aim of sharing lessons learnt. Contributions to this session were welcome by academics working on research projects with industrial partners who have driven experimental evaluations of research outcomes and prototypes with the help of real-world data, or have validated hypotheses by performing surveys and interviews.

For this special session, we finally accepted five contributions involving four universities together with six different companies and research centers. Each of the following sections will address a specific contribution for the special session.

More specifically, the rest of this paper is organized as follows: Section 2 provides an experience report on the usage of serious gaming for training infrastructure operators; Section 3 describes an experience of integrated safety and security management in the chemical and process industry; Section 4 addresses risks related to the cyber-economy for energy suppliers; Section 5 addresses an experience report related to intrusions in power distribution SCADA systems; Section 6 describes a novel industry concept known as smart troubleshooting with interesting IoT applications; and, finally, Section 7 draws conclusions.

2 Using serious gaming to train operators of critical infrastructure

This section presents the development of a serious game component used to train operators of critical infrastructure. It describes the basic operation of the game and how an iterative development process ensured that the pedagogical objectives were met. Lessons learned while developing and testing the game are also presented.

2.1 Introduction

When a new course to train operators of critical infrastructure to use security controls was developed at the Swedish Defence Research Agency (FOI), a serious gaming component was integrated into the course schedule. The purpose was to create a story-living experience, as described by Perla and McGrady [1], which enhances the learning process by allowing the course participants to work with the knowledge gained during the lectures and the laboratory sessions. In the game, the participants have to protect an IT environment of a fictitious company.

Here, the term *serious gaming* is used to describe *a game in which education is the primary goal, rather than entertainment*, as defined by Michaels and Chen in 2006 [2]. The decision to develop the game was made during the overall design of the training course. The game runs as short sessions throughout the course where each session focuses on the security controls presented in the foregoing lectures and labs.

During the development, a board game form factor was used which allowed the design team to focus on the game play rather than on technical solutions. An iterative development process was used with four test runs involving two groups of FOI personnel and two groups consisting of the intended target groups of the training course. After each test run, feedback was collected upon which the design team made relevant adjustments prior to the next test.

2.2 The narrated scenarios and the game play

During the game, the participants are divided into teams of three or four. To create a relevant narrative as described by Perla and McGrady [1], each team constitutes a group of consultants hired by a fictitious company operating a critical infrastructure. The board of executives of the company recently identified that their business falls under the EU directive on the security of network and information systems (NIS Directive) [3]. The task of the team is to ensure that the level of protection of the IT environment meets the requirements of the legislation. Each company has different needs of availability and confidentiality, which means that the groups need to prioritize different security controls.

During each session, the participants must choose a set of security controls to implement in order to handle vulnerabilities and to protect their systems. They can alter the overall design of the IT environment by changing the structure of the network as well as by moving critical systems. The participants also have to manage a series of vulnerabilities. The actions are performed and tracked on a game board having icons that represent the systems. The security controls are represented by playing cards of which only a limited set can be used in each session. Even though the game is not a competition against the other teams, a monetary measurement is used to motivate the teams as described by Sullivan et al. in 2018 [4]. At the end of each session, one or more incidents are played against the IT environments, and if the severity of the incidents surpasses the level of protection, the company will lose some of its revenue.

2.3 Lessons learned

The feedback from the four test groups confirms that the use of serious gaming is a relevant way to train operators of critical infrastructure on cyber security. This conclusion is also supported by observations made by the design team during the tests, where the game engaged all of the course participants. The board game form factor supported vivid discussions within the teams.

During the first three test runs, the narrative was observed to be too weak to be engaging. This issue was solved by adding the NIS directive and the consultant perspective to the narrated scenarios. Another observation was that the initial amount of information early in the first two sessions was too large for the teams to manage. This was solved partly by simplifying the game play and partly by distributing the information more evenly between the sessions.

Future development will add better support for calculating the security levels of the IT environments and to visualize the performance of each team. The tests indicate that the security controls and the cyber incidents are relevant, but further effort is needed to ensure that the game remains relevant.

3 SAFeRA 4STER: Integrated Management of Safety and Security Synergies in Seveso Plants

The Chemical and Process Industry, due to the use of hazardous materials and to the role it plays in the economy, is vastly deemed to be a vital sector and thus considered as a Critical Infrastructure. In order to reduce the risk of failures and minimize the consequences of possible events, the European community created and implemented safety policies and standards such as the Seveso Directives [5] [6]. However, security measures fall outside the scope of the previous version of such regulations and only in the Seveso III Directive they have been partially included. As highlighted in the SAFeRA 2018 call for proposals [7], the security of Seveso sites has become a matter of increasing concern due to growing threats stemming from terrorism, internal malevolence and cyberspace.

3.1 Objective

The objective of the 4STER project [8] is to suggest solutions for managing safety and security in a coordinated manner, as well as to examine how the threats stemming from digitalization are understood and identified. The following three Research hypotheses are defined: 1) Despite tensions, significant synergies between safety and security management exist; 2) Security-related scenarios concerning intentional acts are not adequately considered in documentation following up the Seveso Directive; 3) Many companies in the European process industry lack adequate cyber security awareness. The project will analyze how safety and security can be combined in an integrated approach for securing plants; it will investigate how cyber-physical threats are perceived; and it will suggest methodologies for identifying the indicators of imminent major accidents.

3.2 Relevance and Impact

The project will have three main contributions: 1) drawing an integrated safety and security management framework for Seveso sites; 2) providing deeper insights into attitudes, awareness and preparedness of European process industries in relation to cyber-physical security threats, which are not adequately dealt in Seveso Directives and safety reports; 3) Producing guidelines for the early identification of accident scenarios with intentional causes that allows an easier integration of the safety reports with security-related scenarios. These results will serve for significantly improving safety and security in the 12.000 Seveso III sites of the European Union (http://ec.europa.eu/environment/seveso/). Moreover, regulators, senior managers, safety/ security experts, shop-floor workers in companies, and policy makers benefits from the results, which will be disseminated via seminars, blogs and events by the SAFERA platform.

4 Recent Trends in Cyber Economy and their Impact on Operational Technology

The experience report included in this section addresses the recent trends in cyber economy, summarized under the term ”digital transformation”, from the perspective of an energy supplier. An overview of changes, impacts and some ideas on how to survive in a multicloud universe are given.

The typical functioning of an energy supplier requires the production, transport, supply, trading and sales of energy. These five main parts of one company need to work together but they have widely different characteristics. Energy production, transport and supply are typical parts of the critical infrastructure. For energy transport and supply a grid is needed; the business of an energy distributor is more decentralized. The business of energy trading and sales is depending on data and information technology (IT). While trading operating at stock markets is regulated like banking business, energy sales has a distributed character. Sales agents, partners and being close to their customers dominate this business.

In the last few years some fundamental changes hit the energy suppliers: the liberalization of the energy market. They had to take out the energy transport section due to unbundling reasons. The end of nuclear power usage in Germany took out another stabilization factor. The grow of renewable energies spread our business all over the country. Energy production on the consumer side added more distributed micro-scenarios.

Low market prices for energy forces us to look for new business opportunities. In this segment they meet web companies and start-ups as aggressive competitors.

Due to the changes in the energy market and the impacts of the digital transformation[1] we are urged to move into a future digital market. This urge did not occur solely in our IT department but in any part of our company. Looking for a digital solution in the age of omnipresent easy-to-rent cloud services any part of our company will find something suitable. As outcome our landscape is covered with a lot of cloud solutions. Since most parts of our business cannot be done in isolation - things are interconnected and need to exchange data - we get into a complex interlinked meshed situation, a grid of data and control, spanning through a public shared medium called ”internet”[2]. Further, this expansion of the existence of our company over the internet and clouds is not only virtual.

[1] The term is quite modern in economy, widely used in business and especially in consulting. A number of diverse definitions exist in the literature [9], but a widely accepted one is still to be found.

[2] Anything which uses internet as transport layer can be considered as somehow shared and public. Even if a VPN is used, it will still have the public internet as a base layer.

The internet of things (IoT) is offering even more opportunities. Just get some interoperable IT-gadgets, implement the solution, adapt operational technology (OT) and manage your identities and relations. The IoT, smart devices and any kind of smart technology act as a bridge between the virtual internet and the physical world, thus enlarging the IT network. Many of these new business ideas start as a small proof of concept and there is not enough time to or maybe not the will to waste time in things like enhanced security, administration or compliance. Having real start-ups as competitors a short time to market often dominates the action. At least we cannot slow down to a speed we were used to since the electrification took place [3].

To have a meaningful example for digital transformation at an energy supplier we will take a closer look at the maintenance of wind power stations. Wind farms are under permanent physical stress, so they need maintenance on a regular base. In the past we did the necessary registration of the inventory, checks and maintenance work locally. Operational information technology and office information technology where clearly separated. Today remote checks and control of power plants is common. External and internal staff is using a mixture of office IT and OT to do their job. Manufacturers of OT equipment modernize their technologies and adapt or enable IT network protocols to be used as transport layers in OT environments. Office IT technologies get partly mixed into operational IT. Tomorrow we will use IoT-devices in each wind station to measure and check the OT. We will collect a lot of data in real time and send it via internet to big data analytic services in the cloud. Leveraging artificial intelligence techniques on this data and on the results will allow improved predictive maintenance better then before. Our maintenance staff will be automatically managed by a Cloud-IT-System which controls and supports the work forces via smart gadgets via internet. Operational IT, office IT and cloud IT will be interlinked and mixed.

The Digital Transformation shifts our well known conflict situation "IT versus OT" into a three-party-problem: "OT versus on premise IT versus cloud IT". While the gaps between the technologies are closing, the differences regarding the understanding of risks, the handling of failures and consequences and the understanding that staff have of their job are still there. We are addressing these with cross-functional work groups, overall architectural approaches and a group wide program for a cultural shift which is strongly enforced by the top management

5 Intrusion Attempt on the Power Distribution Grid

Digitalization transforms energy companies to IT constellations within the energy sector. The increased level of system-to-system connectivity enables automation and increases efficiency. New business models are being developed that use the inter-connectivity between such systems. Technologies like virtual local

[3] For example, it took from 1922 up to 1925 to build the Schwarzenbach Dam.

area networks, virtualization and cloud platforms are increasingly utilized to reduce hardware, administrative and maintenance costs. This technology change introduces new dependencies into SCADA systems. As availability of these systems is often critical, such dependencies add new risks. SCADA systems now share both computing and network resources with less critical systems. This experience report addresses a real world intrusion attempt utilizing dependencies that in this case would not have been detected without the visibility provided by network monitoring.

5.1 Digitalization

Digitalization means IT-systems, network domains and connected things (IoT) are being connected with each other and thus enabling exchange of data between these entities. The driving forces for this digital transformation are an increased level of automation, improved efficiency and the enabling of new digital services. Out of this transformation new business models are being developed. Traditional energy companies will in the future become IT-cooperation's within the energy sector. Digital systems with different purposes and requirements, like information technology (IT) and operational technology (OT) systems are interconnected. Applications and services that solve a broad range of different tasks share the same computing resources, but also in some cases the same network assets. The security implication of resource sharing is that less trusted applications, services and networks may share the same computing or network resources. This fact may be used to attack critical systems like SCADA networks for power distribution.

Great efforts are being made at many organizations to reduce the burden related to administration of the ever increasing complexity of IT systems. This has introduced virtualization and cloud platforms, which now is common in many origination's IT environments. A typical IT environment today is a hybrid, consisting of a mix of on-site and outsourced IT infrastructures. Sharing resources reduces costs for administration and maintenance. As soon as there is a potential for cost savings or increased profits, a transformation to a new technology cannot be stopped.

5.2 Sharing Resources

The security implications due to the evolution of IT infrastructures into hybrid systems has not been fully addressed in real world systems. Sharing resources in such systems applies to both servers and network appliances. As an example, core functions in our society like our broadband infrastructures share is some cases network assets with SCADA systems for power distribution. The reason for sharing network resources is simple - It's all about cost savings. If we can use the same network switches for a geographically distributed SCADA system with for example a broad-band management network, there is a possibility for significant cost savings. However, shared resources like network assets may increase the attack surface. In the case presented here, sharing network resources increased the attack surface for a SCADA system that is used for power distribution.

5.3 An Intrusion Attempt

Proactive security and the ability to detect threats related to shared infrastructure resources as early as possible is essential. The earlier a threat can be detected, the less risk for serious and costly incidents.

In this experience report, we describe a real-world intrusion attempt and demonstrate the importance of visibility into shared network resources. By monitoring both SCADA and broad-band management network traffic segments in a shared network switch, the attack could be mitigated before it became a direct threat to the SCADA power distribution network.

6 Smart-Troubleshooting in the Connected Society

Today's digital world and evolving technology have improved the quality of our lives but they have also come with a number of new threats. In the society of smart cities and Industry 4.0, where many cyber-physical devices connect and exchange data through the Internet of Things, the need for addressing information security and solving system failures becomes inevitable. System failures can occur because of hardware failures, software bugs or interoperability issues. In cooperation with Sigma Technology AB [1](Sweden), we introduced the industry-originated concept of "smart troubleshooting", that is the set of activities and tools needed to gather failure information generated by heterogeneous connected devices, analyze them, and match them with troubleshooting instructions and software fixes.

6.1 Introduction and Objective

Most of the components in modern computer systems are based on interconnected devices which are manufactured by different vendors. Though many failures within an individual component may be taken care of by their respective manufacturers; it is likely that any other failure between different components in modern computer systems, such as a simple connectivity problem will not be supported by the manufacturers, as it is generally not covered under the warranty. Therefore, due to interoperability issues, it will not be possible to troubleshoot all system failures based on single product information. Instead, a large amount of information sources should be explored to build knowledge about failure modes, causes (intentional and unintentional), consequences, as well as how to diagnose them and finally repair the system. Also, if performed manually, such a process can be highly time consuming and error-prone.

All the above discussion leads us to believe that diagnosing and troubleshooting failures in an IoT system will be a huge problem in the near future which may not be covered by any manufacturer, unless all the entities within the system are manufactured by the same company. In [10] we look through and analyze

[1] https://www.sigmatechnology.se/news/sigmas-notes-disruptive-innovations-in-the-world-around-us/

previous works in the field of diagnosing and troubleshooting IoT systems. Other related concepts such as error prevention also were looked at. Furthermore, we take a step ahead and look for ways through which the IoT system, in case of a failure, can automatically diagnose itself and possibly, also compute a viable antidote which can be applied to the system to fix the problem in real time. This phenomenon of predicting and preventing a fault, or automatically diagnosing and repairing the system in case of an error, and simultaneously learning so that the same error does not occur twice, is termed Smart Troubleshooting. Smart troubleshooting can be categorized into four primary phases, namely:

- Prevention
- Detection & Diagnosis
- Recovery
- Evolution

As can be intuitively inferred, these phases are sequential and recurrent in a connected cyber-physical system. Prevention, as the name suggests, is the ability of a system to prevent a fault before it happens. However, if the fault is somehow activated resulting in an error, the virtue of the system to detect the same and diagnose it so that an appropriate fix can be applied is termed as Detection and Diagnosis. Further, the process of applying the fix is dubbed as Recovery. Moreover, the system should also be able to learn so that the same error could be prevented from happening again. We call this process ”Evolution”.

Based on the discussion and motivation above, we can formulate our research question as *How can we promptly recognize anomalies in heterogeneous connected devices (including Embedded Systems, Cyber-Physical Systems and the Internet of Things), and (semi)automatically apply appropriate troubleshooting solutions based on available information, in order to restore correct system operation, reduce the time-to-repair and the probability of maintenance mistakes?*

6.2 Challenges and Opportunities

It is evident that the problem of smart troubleshooting - although relatively easy to specify - is highly challenging due to its multifaceted and cross-discipline nature, entailing aspects of artificial intelligence, formal modeling and data analytics, in order to support online identification of failure patterns, mine troubleshooting information based on a combination of natural language and machine readable sources, match appropriate solutions to recognized failures, apply those solutions through structured workflow management models and procedures.

This project shows that while there are numerous approaches to tackle issues like Error Prevention, Detection and Diagnosis, Recovery and Evolution for specific domains in IoT, there is no concrete solution or framework for Smart Troubleshooting that can handle all these issues at once, plausibly in the form of a feedback loop [11]. Moreover, as different components in an IoT system fabricate their own event logs, comprehending event logs with diverse formats is an ambitious problem to solve. Even in case of log format standardization, the events and states recorded could differ in each device.

Digital twins is an important concept that can play a pivotal role in troubleshooting IoT systems in the future. It is essentially a virtual representation, or a virtual doppelganger, as termed by IBM, of a cyber-physical asset. It enables the interaction of the application with devices in a consistent manner by providing an appropriate abstraction layer. Digital twins are conceptualized to follow the life-cycle of a device and its associated data. It can also be used to simulate system operation in a specific scenario without actually running the system, in order to anticipate any faults-errors-failures that might occur over time. The simulations can also be ”fast-forwarded” to foresee the effects of updates, repairs, preventive maintenance, and even future threats. Apart from avoiding a failure in an IoT system, using digital twins can also help predict the future, increase the accuracy and reduce costs. Despite those initiatives, digital twins for IoT can still be considered as a ”concept”, and future efforts will be needed to make IoT digital twins a reality. Therefore, we believe IoT digital twins can be a promising research area which is destined to generate key technologies which can effectively support smart troubleshooting.

7 Conclusion

This paper has provided a brief summary of practical experience reports presented at the industry dissemination session of the 14th International Conference on Critical Information Infrastructures Security (CRITIS 2019). Such a session is very important to stimulate discussion about real-world industry needs and how recent research developments can be leveraged in order to tackle current industry challenges in the CIIP area. We believe the diversity of applications included in this session is also essential to foster comparison and facilitate both knowledge and technology transfer across multiple security-critical domains.

Acknowledgement
The work reported in Section 3 was supported by INAIL via the European Safera project ”Management of Safety and Security Synergies in Seveso Plants” (4STER).

References

1. Perla P, McGrady E (2011) Why wargaming works. Naval War Collage Review, Summer 2011, Vol. 64, No. 3
2. Michael D, Chen S (2016) Serious Games – Games that educate, train and inform. Thomson Course Technology, Boston, MA, USA
3. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

4. Sullivan D, Colbert E, Hoffman E, Kott A (2018) Best practices for designing and conducting cyber physical system war games. Computational and information sciences directorate, U.S. Army Research Laboratory, Adelphi, MD, USA
5. Council Directive 82/501/EEC of 24 June 1982 on the major-accident hazards of certain industrial activities, OJ L 230, 5.8.1982, p. 1–18.
6. Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC, OJ L 197, 24.7.2012, p. 1–37.
7. https://www.safera.eu/
8. Integrated Management of Safety and Security Synergies in Seveso Plants (SAF€RA 4STER) project,https://projects.safera.eu/project/21
9. Reis J., Amorim M., Melão N., Matos P. (2018) Digital Transformation: A Literature Review and Guidelines for Future Research. In: Rocha Á., Adeli H., Reis L.P., Costanzo S. (eds) Trends and Advances in Information Systems and Technologies. WorldCIST'18 2018. Advances in Intelligent Systems and Computing, vol 745. Springer, Cham.
10. Caporuscio M, Flammini F, Khakpour N, Singh P, Thornadtsson J (2019) Smart-Troubleshooting Connected Devices: Concept, Challenges and Opportunities. Journal of Future Generation Computer Systems, To appear
11. Fortino G, Russo W, Savaglio C, Shen W, Zhou M, (2018) Agent-Oriented Cooperative Smart Objects: From IoT System Design to Implementation. in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 11, pp. 1939-1956