# Complex Systems - Network Component Security of SCADA Systems

M. Sverko, T. Galinac Grbac
Juraj Dobrila University of Pula, Pula, Croatia
m.sverko@gmail.com, tihana.galinac@unipu.hr

*Abstract* – **Over the past decade the complexity of industrial control systems (ICS) has been increasing rapidly. There are many reasons for this trend considering new technologies that offer a higher level of control and integration. In addition to that, the amount of data generated during the control of the industrial process is growing rapidly, which further generates a huge amount of internet traffic. Consequently, the resulting industrial control systems get more difficult to maintain, more exposed and more vulnerable to internal and external threats. These issues affect almost every component and ensuring adequate level of reliability and security of industrial control systems network components presents the biggest challenge. This paper addresses security issues of the supervisory control and data acquisition system (SCADA) network component as a complex system and some of the best practices in the application of security guidelines of relevant institutions. In order to provide a basic understanding of the industry-specific environment from a security point of view, we will first give a brief overview of the ICS system as the wider SCADA system working environment, with a focus on core functions and quality requirements. We will further address SCADA system vulnerabilities, threats and protection methods. Finally, we will provide recommended protection and prevention strategies with an example of implementation.**

*Keywords – complex; industiral; system; ics; scada; network; safety; vulnerability; threats; cybersecurity;*

## I. INTRODUCTION

Since the continuity of the production process is the basic requirement for the survival of any industry, clearly all available solutions will be applied to achieve this goal. This inevitably leads to the implementation of new technology solutions and thus resulting with a high degree of dependence of the industrial automation IT layer. It is obvious that this development raises additional security issues that have not been considered in the field of industrial processes so far, and which goes far beyond the domain of physical protection of people and property. This becomes particularly critical with the expansion of computer networks and merging of previously separate production and corporate networks, which for the first time directly expose the industrial plant information system to external threats. Because of such development, it would be logical to expect that, appropriate cyber – information - internet security measures related to the security of industrial control systems will be applied. However, even though until recently the production network component of the ICS was entirely based on open protocols, such an approach was missing. One of the main reasons for this is the belief that these are specific industry protocols and systems that are not the usual targets of cyber-attack documented so far, which were in principle aimed at stealing personal data, credit cards, identities, impersonation, etc. This perception of ICS and such an approach have changed radically over the past decade in which serious and sophisticated cyber-attacks on ICS have been reported with significant consequences. It is not a surprise, given that the control of industrial plants today relies almost entirely on IT support and their security becomes a strategic issue of national interest. Analyzing some of the well-known cyber-attacks of the last decade, such as BlackEnergy3 malware - Ukrainian power grid crash (2015) [1], Stuxnet - attack on Iranian nuclear facilities (2010) [2], Triton malware - Petrochemical plant in Saudi Arabia (2017) [3] and similar, it becomes clear that the sophistication of the algorithm and the required level of knowledge from multiple areas, is not the work of individuals or smaller groups, but more likely, an interference of state-level controlled organizations. Fortunately, some of the relevant international institutions and organizations have been actively involved in developing methods of prevention and defense against these attacks, which has resulted in concrete measures and guidelines for building and maintaining more secure ICS, and especially it's network component. Further content implies the reader's basic knowledge of the computer systems security concept, as well as a general perception of the industrial process, and the role of IT support.

## II. INDUSTIAL CONTROL SYSTEMS (ICS)

There are several definitions of an Industrial Control System, but it mainly implies a term that describes the integration of hardware and software with a network component to support the critical infrastructure and used to control an industrial process. Depending on the industry, each ICS operates differently with significant level of customization, and it was built with the goal of performing tasks efficiently and effectively. In general, the Industrial Control System usually implies distributed control system (DCS) that consists of supervisory control, data acquisition (SCADA), and operational technology (OT) systems that, with a certain degree of interoperability and integration, controls a particular production process, and to some extent (depending on the reach and branching of the system) provide data to higher systems in the corporate network to support business process.

Fig.1 shows ICS as a combination of two networks (supervision and production) that separates direct production process control from production monitoring at the SCADA level.

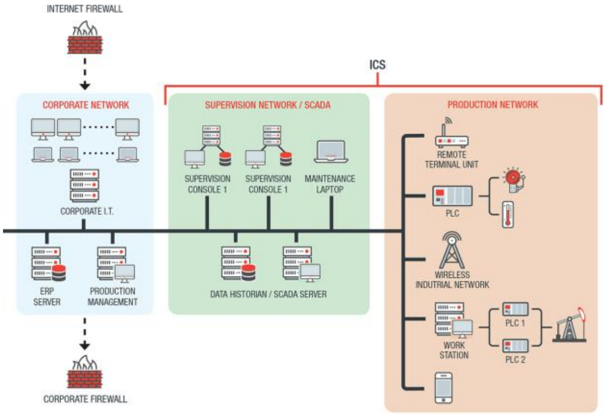


Figure 1. Industiral control system [1]

The Industrial Control System shown on Fig.1 is further logically subdivided into levels according to its role in the business process. Such a division has no strictly defined boundaries, which is understandable given the impact of new disruptive technologies, and the speed of its implementation in the field of industry.

## III. SCADA SYSTEM SECURITY CHALLENGES

The SCADA belongs to the systems that are evolutionary developed following product line concept [4] and is essentially difficult to model due to its interdependence, relationships, different types and levels of interactions between components and with the environment. These present main challenges from the cybersecurity point of view.

### A. *Interconnections*

When it comes to the cybersecurity aspect of the SCADA system, most of the vulnerabilities and threats arise from numerous interconnections. External connections to other systems are easily visible even from simplified network diagrams such as the system division shown in Fig. 1. However, for a more comprehensive understanding, it is necessary to explain the connections within the system itself. Fig. 2 shows a SCADA system decomposed into basic functions and functionalities from the aspect of internal and external connections.

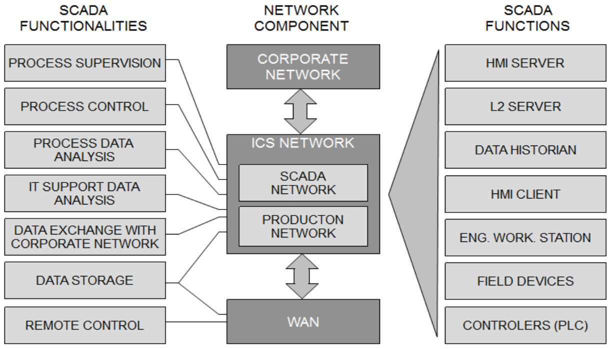
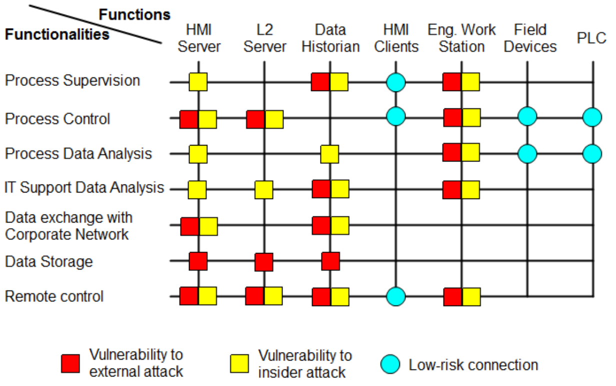


Figure 2. SCADA system decomposition and interconnections

The division was performed by adapting the functional concept ontology and function, behavior, state (FBS) model [5],[6]. In this interpretation, functionalities refer to activities that can be performed within the system, i.e. according to T.J. van Beek and T. Tomiyama [6] "*a description of behavior recognized by a human through abstraction in order to utilize it*", while functions represent objects that enable the realization of functionality. The connection between functionality and function answers the question of what to do and how to do it.

Generally, it gives an idea of complexity on example of numerous interconnections between various functions and functionalities within the SCADA system. Given that the logical connections between objects in the image are in fact physically realized through the SCADA network component, which as part of ICS network is further exposed to the corporate network and WAN, it becomes clear that the network component of the SCADA system is extremely vulnerable to external and internal attacks of any type.

Considering previous SCADA system decomposition into functions and functionalities, Fig. 3 shows the critical connections on which internal and external threats can be realized.



| Functions<br>Functionalities | HMI Server | L2 Server | Data Historian | HMI Clients | Eng. Work Station | Field Devices | PLC |
|---|---|---|---|---|---|---|---|
| Process Supervision | 🟨 | | 🟥🟨 | ● | 🟥🟨 | | |
| Process Control | 🟥🟨 | 🟥🟨 | | ● | 🟥🟨 | ● | ● |
| Process Data Analysis | 🟨 | | 🟨 | | 🟥🟨 | ● | ● |
| IT Support Data Analysis | 🟨 | 🟨 | 🟥🟨 | | 🟥🟨 | | |
| Data exchange with Corporate Network | 🟥🟨 | | 🟥🟨 | | | | |
| Data Storage | 🟥 | 🟥 | 🟥 | | | | |
| Remote control | 🟥🟨 | 🟥🟨 | 🟥🟨 | ● | 🟥🟨 | | |

🟥 Vulnerability to external attack 🟨 Vulnerability to insider attack ● Low-risk connection

Figure 3. SCADA system critical connections respecting cybethreats

### B. *Quality requirements*

Depending on the relevant institution, there are several definitions of quality. According to ISO [7], quality is a set of properties and characteristics of products, processes and services that relate to the ability to meet an identified need, or one that is implied. The IEEE definition has a similar meaning, according to which it is the degree to which a system, component or process meets user needs and expectations. Accordingly, the observed system, i.e., the network component of SCADA has the following key quality requirements:

- Stability - from the perspective of the SCADA network component, it is a property that allows the controlled process to operate in given parameters without critical deviations that can destabilize the component, and consequently, the whole system.

- Reliability - in general, it is a property of a system to generate expected output parameters for certain input parameters at a given time. In the domain of SCADA system, it is achieved primarily by applying mechanisms, procedures and tools that are in the function of detecting and preventing hardware and software failures, in addition to controlling the amount of traffic and monitoring throughput.

- Availability - implies the probability that the system will be operable at the time of need. This feature for a given system is measured as the time of unavailability, i.e., days per year when the system was available with reduced functionality/ capacity or was not available/operable at all (down days). Associated with this feature is the term “high availability”, which stands as a collective name for various methods and ways to achieve a higher level of system availability. In the case of computer support systems, this includes solutions such as network topological configurations, server redundancy, network components, power supplies, and similar.

- Security - from a broader point of view, in the domain of industrial automation, security implies prevention of (intentional or unintentional) interference with the performance of certain operation of the control system that monitors the controlled process. At the level of the SCADA system network component (with exception of possible physical damage) this mainly implies cybersecurity.

- Response time - implies the total amount of time it takes for the system to respond to a certain request. Within the network component of SCADA system, this mainly refers to the velocity of data exchange at the HMI-PLC level, and PLC-instrumentation. This enables the timely receipt of critical information from the field (actuators, sensors…), to the controller, and forwarding to the HMI. In the opposite direction, timely feedback control signal generated from the HMI is insured. Another example would be real-time archiving, which ensures the possibility of useful analysis supporting requirements of various subsystems (maintenance, planning, IT support, management).

## IV. SCADA SYSTEM SECURITY

Determining SCADA system vulnerabilities is a significant help to system integrators in defining key system points where the risk of exploiting vulnerabilities can be reduced, and an attack neutralized.

### *A. Users*

From security point of view, one of the main issues resides in number and types of users accessing devices across the networks. Even relatively simple SCADA system is accessed by number of various types of users on daily bases. Some of these users are poorly educated in terms of cyber security, and their access rights are usually much higher from the actual requirements.

TABLE I. SCADA USERS AND ACCESSED NODES

| **SCADA users reach** | | |
|---|---|---|
| ***User role*** | ***Access node*** | ***Task*** |
| HMI operator | HMI Client | Process monitoring and control |
| Maintenace | PLC, Field devices, Eng. work st. | Hw/sw modification, data analysis |
| Management | Data historian, remote connection. | Data analysis, process monitoring |
| IT support | Servers, Network infrastructure, virtualization | Software modificaton, database maintenance, network devices configuration, data analysis |
| Process ing. | HMI Client, Data historian | Data analysis, process monitoring |
| Supervisor | HMI sever, HMI client, Data historian | Process monitoring and control, data analysis |
| Trusted contractor | Servers , Eng. work st., HMI severs, PLC, Field devices | Hw/sw modification, network devices configuration, data analysis |

### *B. Vulnerabilities*

Common elements and causes of vulnerability:

- external support and contractors - Since such companies are not subject to internal security policies, in case their local network is compromised, there is a risk of infiltration into the ICS network, and even OT network (in case of direct connection to one of the field devices or PLC). One of the protection methods is a VPN connection. This will not eliminate the threat but can greatly reduce the range of a possible attack.

- Weak network segmentation - Insufficiently separated IT and OT networks is one of the factors that often results in compromised ICS. Poorly defined access control can allow computers on an IT network to access devices on OT network, making it possible to directly interfere with execution of a controlled process. This way, possible malicious infiltration from the level of the IT network can easily spread to all devices located in the OT network, and such devices have weak to non-existing protection against cyberattacks.

- Default configurations - When configuring the SCADA system, it is common practice to leave the default factory settings of communication parameters (usernames, passwords, IP addresses etc.), so that the various maintenance teams have easy access for future modifications and system upgrades. This often happens during the commissioning phase, and usually under the assumption that ICS network is well protected and has no direct access to internet. Sometime this practice can even be supported by the client with the intention of complete isolation of ICS network. Such a network structure, however, can easily change, making the devices on it very exposed.

- Open protocols - industrial protocols were not designed with security in mind. Although this is changing with the introduction of new generation protocols, older SCADA systems mostly work on open protocols such as the universally present MODBUS, without the possibility of encryption and data protection.
- Vulnerabilities in customized applications - many applications that are used exclusively in the field of industrial automation are developed in small series and are often specially tailored to specific customers for specific purposes. This results in applications that are not sufficiently tested against operating system security patches, and do not have the required level of protection implemented. Also, such applications are almost never updated. This results in a whole range of vulnerabilities to various attacks such as SQL Injection, Command Injection, Parameter manipulation. credential sniffing.
- Lack of safety awareness - due to insufficiently developed norms and procedures for achieving a satisfactory security level, employees can easily become victims of social engineering, phishing, spear phishing and similar attacks that exploit the ignorance of users, and use their access rights to infiltrate to the network.

### *C. Threats*

Given the previously explained vulnerabilities of the SCADA system, the realization of the following threats is possible:

- Malware - a key problem with such threats is the ability to expand regardless of network-level protections if they can be physically transmitted through removable media. One example is Stuxnet malware, which entered the Siemens network via an infected USB key, and which was spread to the local network by an employee from his laptop.
- Insider attack - this kind of attack mostly happens unintentionally by employees due to ignorance of previously discussed safety procedures and rules in combination of authorized system access.
- Denial of access (DoS/DDos) - It is an attack on network connections by sending multiple requests to the attacked resource with the aim of exceeding the capacity to handle them. In the case of SCADA systems, this can interfere with real-time communication between components crucial for control and execution of the process. One of the extreme cases would be a massive attack on PLC ports which could result in a blockage of PLC operation and thus a complete loss of process control.
- Third-party threats - with the growing level of complexity of ICS, and the common practice of outsourcing major tasks in building and maintaining the systems, the level of threats that come with computers and computer components connecting from outside the ICS rapidly increases. An additional risk is posed by virtualization solutions that enable multiple virtual machines to be connected to a local network form single physical node.
- Technical and physical malfunctions - mechanical failures of network components, cables, computer components, and power outages can lead to temporary downtime, or complete interruption of the controlled process. Standard procedure to prevent this type of threat is a maintenance plan that targets to replace components before the end of their life cycle or introduces redundancy in the segment crucial to the continuity of the process.

### *D. Methods of protection*

Fortunately, most of previously addressed vulnerabilities, and the threats that these vulnerabilities can exploit, have known and elaborated methods and defense procedures, most of which are already implemented while designing architecture and building systems. Following are some recommendations:

- Virtual patching - the SCADA system as an IS has certain particularities that arise from the field of application. Some of these specifics require special care and planning when applying security patches to avoid possible downtime that could potentially occur. Such an approach, while necessary, may ultimately result in too late protection of the system from new threats. Virtual patching is a method that applies a security patch at the network level, thus neutralizing a potential threat before the hardware/software component itself. The method is also known as proximity control because it blocks the threat before it was able to exploit the vulnerability of the final target.
- Network segmentation - partitioning a network into segments is a comprehensive approach that protects entire subsystems, and it is standard recommendation of multiple reference organization like NIST, ENISA, US department of homeland security and others.
- Security measures between ICS and the corporate network - the key point of protection of all subsystems at the level of the ICS network is the access point to the corporate network. An already adequately configured firewall will prevent the attack from spreading laterally from one network to another.
- Authorizations and user accounts - proper configuration and regular application of recommended protection measures at the level of user identification, authorization and authentication has a significant impact on cyber threats realization, in addition, physical access restriction of unauthorized persons to key resources of the SCADA system is highly recommended but often avoided practice.

- Protection at the level of computers used for system configuration (Endpoint protection on engineering stations) - each SCADA system has a workstation that contains various configuration software, as well as entire development interfaces for modifying and developing existing applications, PLC programs and HMI interfaces. The security of such workstations is crucial, as they have access to critical system components. The usual protection of such workstations refers to the presence of software packages: antivirus, anti-spyware, personal firewall, application control, encryption, intrusion detection tools etc.

- Reduction of multi-purpose SCADA components - it is often the case that individual workstations are used for several different purposes, and thus have access to various critical components of process control. It is recommended that such computers should be reduced to a single purpose, or at least the smallest possible number given the actual requirements. This will ultimately increase the number of workstations on the network but will also increase the level of security.

- Disabling USB ports - although this measure is seemingly unnecessary, since SCADA users should be sufficiently educated and responsible to take care of how to use external devices, USB sticks are one of the most common attack vectors that are easily overlooked by users

## V. Recommended strategies

As previously stated, multiple national and international institutions are involved in the issue of protection and prevention of ICS attacks. Some of the major guidelines were defined during 2015, which provide concrete and specific measures aimed at increasing the degree of ICS security [9]. That same year, the U.S. Homeland Security, in collaboration with the FBI and NSA issued following recommended strategies in order to protect ICS networks [8].

- Implement application whitelisting.
- Ensure proper configuration/patch management.
- Reduce your attack surface area.
- Build a defendable environment.
- Manage authentication.
- Implement Secure Remote Access.
- Monitor and respond.

It is estimated that these measures, if published earlier, could have prevented significant number of the security incidents reported to the Industrial control systems cyber emergency response team (ICS-CERT) in the year before. Fig. 4 Shows percentage of ICS-CERT reported Incidents for year 2014 and year 2015 potentially mitigated by each strategy [8]. It is obvious that patch management is the most critical strategy, i.e. the largest number of reported security incidents refers to this segment of security. According to this criterion, the second most important ICS protection strategy is attack surface area reduction. By focusing on just those two components of cyberattack prevention, the total number of recorded incidents would be reduced by 45 percent. Potential attack in both categories can be prevented by applying only two protection methods that refer to regular security updates (or virtual patching), while the other is network segmentation.

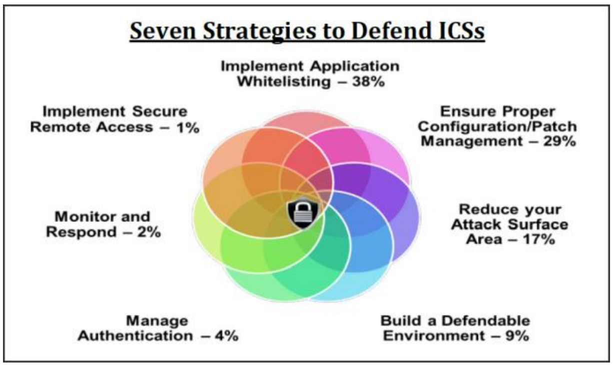


Figure 4. Percentage of ICS-CERT for yewr 2014 and 2015 incidents potentially mitigated by each strategy [8]

## VI. Example of network segmentation

The key decision in network segmentation is the choice of resources to be included within a network segment. The number of different subnets from which they are accessed is a crucial information in making this decision.

Fig. 5 shows ICS network separated from the corporate network with the application server and data historian located within the corporate network. This can be a logical choice, as these nodes are accessed for business data analysis within the same network. However, data for this is provided by nodes located in the control network and setting up just one firewall is not enough to prevent the spread of attacks to both networks.

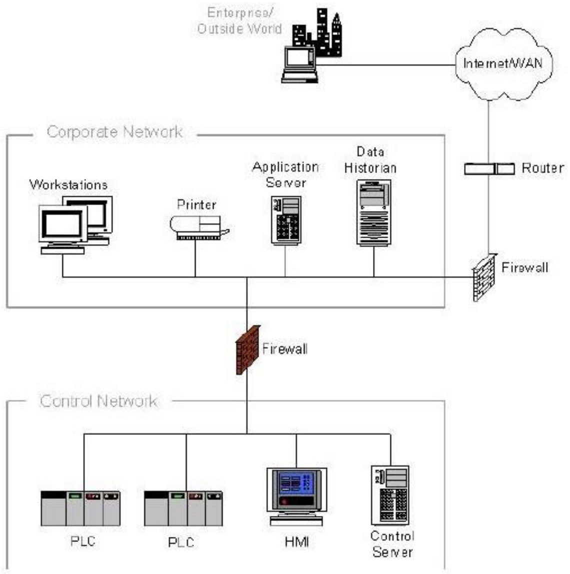


Figure 5. Network segmentation with firewall [9]

As previously shown in Fig. 3, data storage interconnects with HMI server, L2 server and data historian. All these connections are vulnerable to external attacks if trusted connections form Data historian are coming from corporate network with internet access. This issue is even more emphasized by application server exchanging data with HMI server (data exchange with corporate network functionality).

While this solution will reduce the possibility of the attack spreading laterally from one network to another in case it is coming from nodes on the corporate network, it will not be effective in case application server and data historian are already infected. There is still a possibility of malware spreading or DoS/DDos attacks reaching as far as the production network.

Further improvement is achieved on Fig. 6 by implementing demilitarized zone (DMZ) which provides an additional communication restriction where devices respond only to a pre-configured set of communication requests. Separating the Application server and Data historian by installing firewalls that support DMZ forms a firewall pair separating the corporate and control networks twice. Considering critical connections and threats form Fig. 3, this solution eliminates all direct vectors of internal and external attacks coming from the corporate network. There are no trusted connections between corporate and supervisory networks i.e. no attack or malware spreading can break through both firewalls with different sets of rules. There is still the question of remote connections directly accessing ICS network as shown by remote control functionality in Fig. 2.

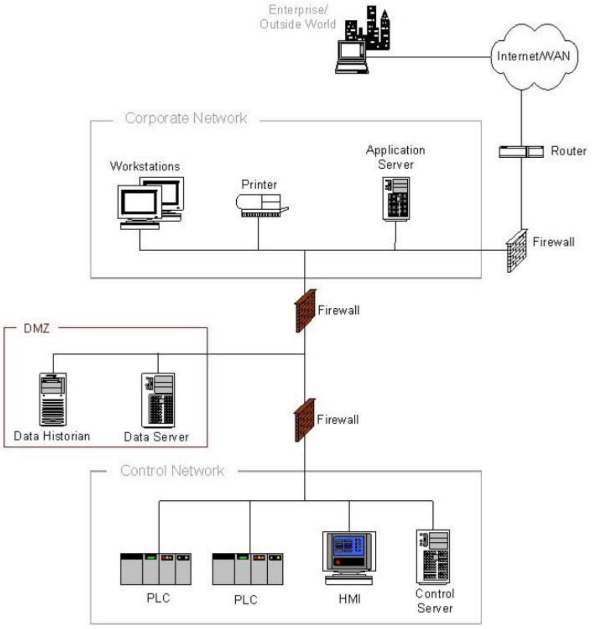


Figure 6. Network segmentation with DMZ [9]

## VII. Conclusion

In this paper, we have addressed industrial security challenges that particularly affect the SCADA system and network component arising from a high level of interconnection within the system as well as with the environment as a result of general quality requirements. Vulnerabilities, threats and methods of protection were defined accordingly, respecting specific user behavior, network structure and protocols, customized software and specific hardware elements affecting SCADA system cybersecurity.

The success of the applied strategies largely depends on the understanding of industry specific security challenges, quality requirements, user safety awareness, vulnerabilities and available methods of protections addressed in this paper.

## Acknowledgment

This paper acknowledges the support of the Croatian Science Foundation under the project HRZZ-IP-2019-04-4216, and the support of the Erasmus+ Key Action 2 (Strategic partnership for higher education) project No. 2020–1–PT01–KA203–078646: "SusTrainable - Promoting Sustainability as a Fundamental Driver in Software Development Training and Education". The information and views set out in this paper are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

## References

[1] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems," in *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, Sep. 2020, vol. 2020-Septe, pp. 1537–1543, doi: 10.1109/ETFA46521.2020.9212128.

[2] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON Proceedings (Industrial Electronics Conference)*, 2011, pp. 4490–4494, doi: 10.1109/IECON.2011.6120048.

[3] A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The First ICS Cyber Attack on Safety Instrument Systems Understanding the Malware, Its Communications and Its OT Payload," *Black Hat USA*, 2018.

[4] T. Galinac Grbac, "The Role of Functional Programming in Management and Orchestration of Virtualized Network Resources Part I. System structure for Complex Systems and Design Principles," no. 2017, pp. 1–35, 2021, [Online]. Available: http://arxiv.org/abs/2107.12136

[5] T. J. van Beek and T. Tomiyama, "Requirements for complex systems modeling," *18th CIRP Des. Conf. …*, no. February, 2008, [Online]. Available: http://esi04.campus.tue.nl/publications/darwin/2008_15_vBeek_Tomiyama_CIRP.pdf.

[6] T. J. Van Beek and T. Tomiyama, "Integrating conventional system views with function-behaviour-state modelling," *Compet. Des. - Proc. 19th CIRP Des. Conf.*, no. March, pp. 65–72, 2014.

[7] "ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary." https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en (accessed Apr. 20, 2021).

[8] US Homeland Security NCCIS, "Seven Strategies to Defend ICSs," pp. 1–7, 2015.

[9] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2," *NIST Spec. Publ. 800-82 rev 2*, pp. 1–157, 2015, [Online]. Available: http://industryconsulting.org/pdfFiles/NIST Draft-SP800-82.pdf.