Enhancing Attack Resilience by Protecting the Physical-World Interface of Cyber-Physical Systems

Rainer Falk, Steffen Fries
Corporate Technology
Siemens AG
Munich, Germany
e-mail: {rainer.falk|steffen.fries}@siemens.com

***Abstract*—Cyber physical systems operate and supervise physical, technical systems using information and communication technology, also called Operation Technology (OT). Cyber security solutions focus on the OT part, i.e., on the information and communication technology. The focus of cyber security is protection, detection, and respondence to cyber attacks. Cyber resilience aims at delivering an intended outcome despite attacks and adverse cyber events and even failures not directly related to attacks. Protecting the link between the control systems and the physical world, has been addressed only in some very specific cases, e.g., charging of electric vehicles. We propose a physical-world firewall that limits the impact on the physical world of a successful attack of automation systems, thereby enhancing the resilience of cyber-physical system against successful attacks against its OT systems.**

Keywords–cyber security; cyber resilience; system integrity; cyber physical systems; industrial automation and control system; Internet of Things.

I. INTRODUCTION

The traditional focus of IT security relates to IT-based control equipment and data communication (Ethernet, IP). In addition to this, in OT systems also the field level has to be considered down to the interface between the control system and the physical world via sensors and actuators.

Traditionally, IT security has been focusing on information security, protecting confidentiality, integrity, and availability of data at rest and data in transit. In Cyber-Physical Systems (CPS), major protection goals are availability, meaning that automation systems stay productive, and system integrity, ensuring that it is operating as intended. Typical application domains are factory automation, process automation, building automation, railway signaling systems, and energy management. Cyber security is covering phases protect, detect, and react: Protecting against threats, detecting when an attack has occurred, and recovering from attacks.

We see resilience of cyber-physical systems as an important protection goal, limiting the effect of potential successful attacks on a cyber-physical system in the physical world. It can be rather seen as a strategy than a specific technology. Our objective is to increase the robustness with respect to intentional attacks, although resilience in general would consider also accidental failures.

After giving an overview on cyber physical systems and on industrial cyber security in Sections II and III, a new approach on protecting the interface of a CPS between the cyber-world and the physical world is described in Section IV. It is a concept to increase the resilience of a CPS when being under attack. Aspects to evaluate the new approach are discussed in Section V. Section VI concludes the paper.

II. CYBER PHYSICAL SYSTEMS

A cyber-physical system, e.g., an industrial automation and control system, monitors and controls a technical system. Examples are process automation, machine control energy automation, and cloud robotics. Automation control equipment is connected with sensors (S) and actuators (A), connected directly with automation components, or via remote input/output modules. The technical process is controlled by measuring its current state using the sensors, and be determining the corresponding actuator signals to influence the technical process.

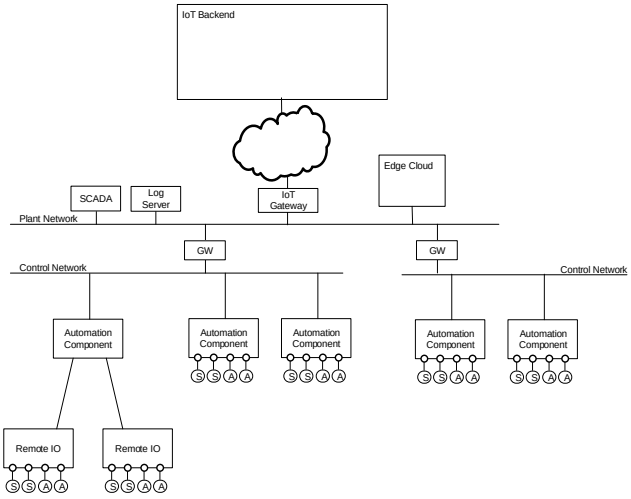

Figure 1. Example CPS System

Figure 1 shows an example of an industrial automation and control system, comprising different control networks connected to a plant network and a cloud backend system. Separation of the network is typically used to realize distinct control networks with strict real-time requirements for the interaction between sensors and actuators of a production cell, or to enforce a specific security policy within a production cell. Such an industrial automation and control system is an example of a cyber-physical system.

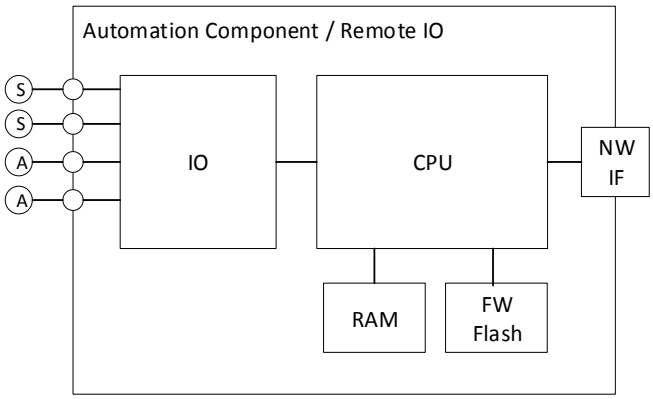

Figure 2. Automation Component

Figure 2 shows the typical structure of automation components. The functionality realized by an automation component is largely defined by the firmware/software and the configuration data stored in its flash memory. In practice, it has to be assumed that each software component may comprises vulnerabilities, independent of the effort spend to ensure high software quality. The impact of a vulnerability in automation equipment does not affect only data on the automation component, but the effect it has on the physical world.

III. INDUSTRIAL CYBER SECURITY

Protecting industrial automation control systems against intentional attacks is increasingly demanded by operators to ensure a reliable operation, and also by regulation. This section gives an overview on industrial security, and on the main relevant industrial security standard IEC 62443 [8] and integrity security requirements.

A. Industrial CPS Security Requirements

Industrial security is called also Operation Technology security (OT security), to distinguish it from general Information Technology (IT) security. Industrial systems have not only different security requirements compared to general IT systems, but come also with specific side conditions that prevent that security concepts established in the IT domain can be applied directly in an OT environment. For example, availability and integrity of an automation system often have a higher priority than confidentiality. As an example, high availability requirements, different organization processes (e.g., yearly maintenance windows), and required certifications may prevent the immediate installations of updates.

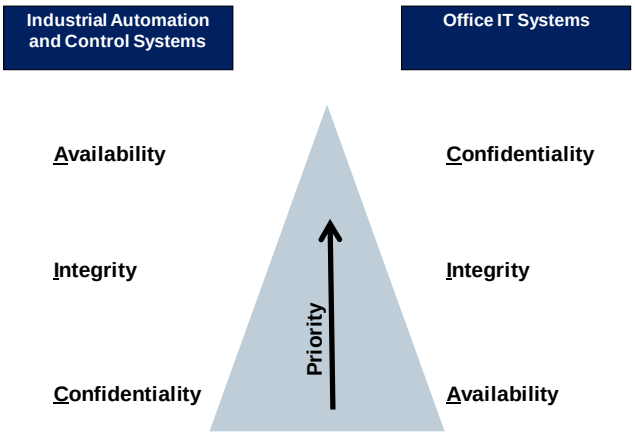

Figure 3. The CIA Pyramid [6]

The three basic security requirements are confidentiality, integrity, and availability. They are also named "CIA" requirements. Figure 3 shows that in common IT systems, the priority is "CIA". However, in automation systems or industrial IT, the priorities are commonly just the other way round: Availability has typically the highest priority, followed by integrity. Confidentiality is often no strong requirement for control communication, but may be needed to protect critical business know-how. Shown graphically, the CIA pyramid is inverted (turned upside down) in many automation systems.

Specific requirements and side conditions of industrial automation systems like high availability, planned configuration (engineering info), long life cycles, unattended operation, real-time operation, and communication, as well as safety requirements have to be considered when designing a security solution. Depending on the considered industry (vertical), they may also be part of the critical infrastructure domain, for which security requirements are also imposed for instance by the European Network and Information Systems (NIS) directive [7] or country specific realizations of the directive. Further security requirements are provided by applying standards defining functional requirements, for instance defined in IEC 62443. The defined security requirements can be mapped to different automation domains, including energy automation, railway automation, building automation, process automation.

Security measures to address these requirements range from security processes, personal and physical security, device security, network security, and application security. No single security technology alone is adequate, but a combination of security measures addressing prevention, detection, and reaction to incidents is required ("defense in depth").

B. Overview IEC 62443 Industrial Security Standard

The international industrial security standard IEC 62443 [8] is a security requirements framework defined by the International Electrotechnical Commission (IEC). It addresses the need to design cybersecurity robustness and resilience into industrial automation and control systems, covering both organizational and technical aspects of security over the life cycle. It is applied successfully in different automation

 ISBN: 978-1-61208-743-6

domains, including factory and process automation, railway automation, energy automation, and building automation. The standard specifies security for industrial automation and control systems (IACS) and covers both, organizational and technical aspects of security. Specifically addressed is the setup of a security organization and the definition of security processes as part of an information security management system (ISMS) based on already existing standards like ISO 27002. Furthermore, technical security requirements are specified distinguishing different security levels for industrial automation and control systems, and also for the used components. The standard has been created to address the specific requirements of industrial automation and control systems. In the set of corresponding documents, security requirements are defined, which target the solution operator and the integrator but also the product manufacturer.

Part 3-3 of IEC 62443 [10] defines seven foundational requirements group specific requirements of a certain category:

- FR 1 Identification and authentication control
- FR 2 Use control
- FR 3 System integrity
- FR 4 Data confidentiality
- FR 5 Restricted data flow
- FR 6 Timely response to events
- FR 7 Resource availability

For each of the foundational requirements there exist several concrete technical security requirements (SR) and requirement enhancements (RE) to address a specific security level. In the context of communication security, these security levels are specifically interesting for the conduits connecting different zones.

Four Security Levels (SL1, SL2, SL3, SL4) are defined that correlate with the strength of a potential attacker as shown in Figure 4. The targeted security level of a zone of the industrial automation and control system is determined based on the identified risk.

4 Security Level (SL)	
SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

Figure 4. IEC 62443 defined Security Level [6]

To reach a dedicated security level, the System Requirements (SR) and potential Requirement Enhancements (RE) defined for that security level have to be fulfilled. The standard foresees that a security requirement can be addressed either directly, or by a compensating countermeasure. The concept of compensating countermeasures allows to reach a certain security level even if some requirements cannot be implemented directly, e.g., as some components do not support the required technical features. This approach is in particular important for existing industrial automation and control systems, so called "brown-field installations", as existing equipment can be continued to be used.

C. *Resilience*

Being resilient means to be able to withstand or recover quickly from difficult conditions [1]. It shifts the focus of "classical" IT/OT security, that puts the focus on preventing, detecting, and reacting on cyber-security attacks, to the aspect to continue to deliver an intended outcome despite an adverse cyber attack is taking place. More specifically, resilience of a system is the property to be resistant to a range of threats and withstand the effects of a partial loss of capability, and to recover and resume its provision of service with the minimum reasonable loss of performance [2]. It has been addressed in telecommunications, ensuring that subscribers can continue to be served even when one line is out of service. Bodeau and Graubart [5] define resilience guidelines for providers of critical national telecommunications infrastructure in the UK.

In a cyber-physical environment, a main objective is to ensure that the CPS stays operational and that its integrity is ensured. In the context of an industrial automation and control system, that means in particular that (only) intended actions in the physical world continue to take place even when the automation and control system of the CPS should be attacked.

IV. PROTECTING THE CPS PHYSICAL WORLD INTERFACE

Well-known IT security technologies like encryption and access control, protecting data at rest, in transit, and partly even data in use. In cyber-physical systems, this is not enough. Also, the interface between the OT part (automation systems) and the physical world has to be protected, limiting the potential danger that an automation system can have on the physical world when it is attacked. A successful attack on the automation system or control network can have an impact on the physical world [3].

This section describes the concept of a "physical world firewall" that limits the access to the physical world from OT automation systems. The objective is to increase the resilience of cyber-physical systems, by limiting the impact of an attacked automation system on the physical world.

A. *Physical-World Firewall*

The main idea is to filter the communication between sensors and actuators on one side, and the control equipment on the other side. This can be called physical-world firewall. It limits in which way a control system, which might be under attack, can impact a physical system in the real world. The filtering takes place directly at the input/output interface, so

that it is independent from the software-based functionality of the automation component.

Similar as a communication firewall for data traffic that analyzes and filters data packets (IP packets and IP-based communication), here the actuator and sensor signals are filtered. The allowed signal ranges and dynamic parameters are monitored and limited.

If the signal filtering policy is violated, the signal cannot be simply dropped like an IP packet. Instead, a replacement signal is provided. The replacement signal may be a fixed default value, or a clipped maximum/minimum value that is within the allowed value range, or it may be an out-of-range signal that will be detected by an actuator as failure signal).

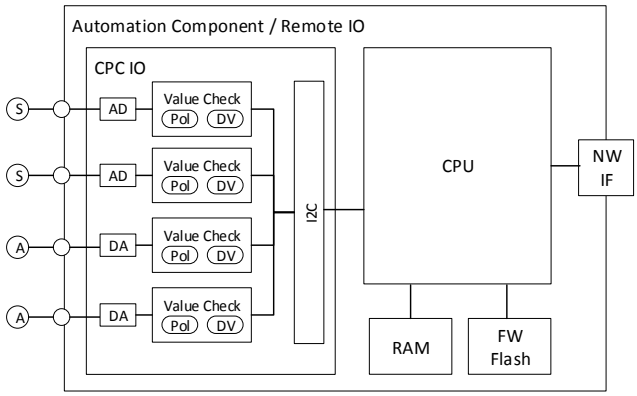

Figure 5. Automation Component with Integrated Physical World Firewall

Figure 5 shows an automation component with an integrated Cyber Physical Controlled IO Interface (CPC IO). The CPU can authenticate towards its CPC IO after a successful self-integrity check. Each input/output channel is monitored separately by the "Value Check" component: It verifies whether the sensor input value or the actuator output value is in the given allowed corridor and thus is compliant with the policy Pol. Besides value range, also statistical parameters and dynamic parameters can be checked. If the policy is met, the value is allowed, otherwise, the configured default value (DV) of provided to ensure the system stays operational. It is possible to lock the input/output interface in the case of a policy violation. The lock may be permanent, or it can be reset at a reboot of by manual user interaction.

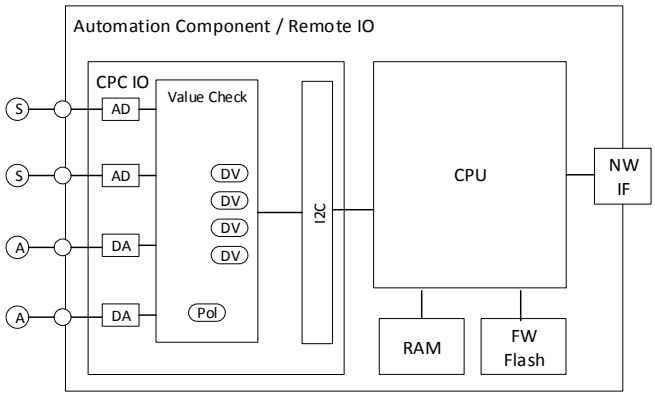

Figure 6. Automation Component with Integrated Physical World Firewall

A different variant is shown in Figure 6, where the signals of multiple input/output channels are checked in combination. This allows to perform cross-checks between sensor and actuator signals. Moreover, if this approach is applied in a distributed system, it allows to take certain properties of potentially different sensors/actuators into account. Specifically, if the sensors/actuators used are a mixture of standard (legacy) and specifically hardened, trusted sensors, a potential security assertion can be used in the evaluation of the signals giving the trusted sensor a higher weight in the evaluation. This is especially advantageous if a larger number of legacy sensors/actuators is already deployed and secure siblings are installed as add-on in a stepwise manner. More information on the basic concept of trusted sensors is described in [6].

B. Dynamic Resilience Management

The policy of the physical-world firewall can be adapted dynamically, depending on the current operating state of the CPS. This allows to restrict the possibility to influence the physical world even more strictly, as the current state of the production system and the currently performed production step, e.g., cooling or filtering a fluid, can be reflected in the current configuration of the physical-world firewalls.

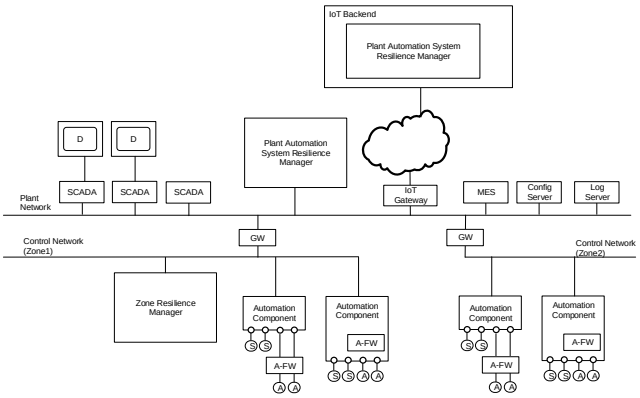

Figure 7. Dynamic Resilience Management

Resilience managers determine the physical-world firewall policy dynamically, depending on the current state and context of the CPS, see Figure 7. They adapt during operation the current policy configuration of the physical-world firewalls.

The policy adaptation performed by resilience managers can use in particular the following information:

– The current state of the physical world, as obtained by trusted sensor nodes [6].

– The current production batch, the current production step, operating state (e.g., standby, preparation, active, service, alarm). In real-world deployments, the information may be obtained from a Manufacturing Execution System (MES).

– Cyber attacks detected by an integrity monitoring system or an intrusion detection system, supervising the CPS.

 ISBN: 978-1-61208-743-6

C. Authenticating Physical Signals

In data communication, the sender of a data packet can be identified by an identifier, e.g., an internet protocol (IP) address or a media access control (MAC) address. The sender may be authenticated cryptographically. A data firewall can filter data packets depending on address information and content.

In a physical world, the source of a signal can in general not be identified by an explicit identifier, included in the data communication. However, it is usually possible to identify the source implicitly based on the cabling.

A higher level of confidence can be achieved by performing signal authentication. The sender of a signal can be identified by a sender-specific fingerprint information, e.g., a noise signal. Furthermore, it is possible to actively add a signal marker (signal watermarking), e.g., a coded spread-spectrum signal [14][15][16]. This allows to identify the source of a signal by evaluation properties of the signal.

V. EVALUATION

The security of a cyber system can be evaluated in practice in various approaches and stages of the system's lifecycle:

- Threat and Risk Analysis (TRA or TARA) of a cyber physical system (for a system being under design or in operation). In a TRA, possible attacks (threats) on the system are identified. The possible impact and probability are evaluated to determine the risk of the identified threats.
- Security checks can be performed during operation or during maintenance windows to determine key performance indicators (e.g., check for compliance of device configurations).
- Security testing (penetration testing) can be performed for a system that has been built, but that is currently not in operation. The system is attacked by "white hat" hackers to identify vulnerabilities that need to be addressed.
- Security testing can be performed also on a digital representation of a target system, e.g., a simulation in the easiest case. This allows to perform pentesting for systems that are not existing yet physically (design phase), or to perform pentesting of operational systems without the risk of disturbing the regular operation of the real-world system.

A holistic protection concept has to address measures for protect, detect, and react. No single measure or security technology alone can result in an adequate security level. It is always a set of measures that, when used in combination, can bring down the risk to an acceptable level.

The security measures presented in this paper, acting on the interface between the cyber world and the physical world, provide an additional security measure that can be used as part of a defense-in-depth security concept. It is complementary to well-known security measures that focus on the IT/cyber part. The protection is complementary, as it operates directly at the interface towards the physical world, not on computer-based control functions as conventional IT security technologies. Even if all security measures in the pure IT/cyber world fail, still the impact on the physical world can be controlled. It can serve as "last line of defense", allowing to connect cyber systems from the physical world in a tightly controlled way, or even disconnecting some automation systems from the physical world when needed.

As long as the proposed technology has not been proven in real-world operational setting, it can be evaluated conceptually by analyzing the impact the additional measure has on the identified residual risks of a TRA. A TRA identifies threats against a system, and determines the risk depending on probability and impact. The general effect of the presented security measure is that the impact of a threat on the physical world is reduced. Whatever attack is ongoing on the automation and control system, still the possible impact on the real, physical world is limited. So, the measure helps to reduce the risk of threats having an impact on the physical world. However, TRAs for real-world CPS are not available publicly. Nevertheless, an illustrative example may be given by a chemical production plant performing a specific process like refinery, or a factory producing glue or cement. If the plant is attacked, the attack may target to destroy the production equipment by immediately stopping the process leading to physical hardening and thus to a permanent unavailability of the production equipment. In this case, trusted sensors could be used to detect a falsified sensor signal, and the physical-world firewall can be used to limit actions in the physical world. Thereby, a physical damage of the production equipment can be avoided. If needed, a controlled shutdown of the production site can be performed.

A major advantage of the physical-world firewall is the property that it can be added to existing brownfield deployments. Legacy equipment, may be 10 or even 20 years old, not even been designed with security in mind, and without getting patches. In such cases, the physical-world firewall can be used as an "add-on" security measure for an existing CPS. It can be used as compensating countermeasure to address security requirements defined by industrial security standards like IEC62443-3.3 [10], where conventional cyber security measures cannot be deployed. However, it can be used also as additional layer of defense in CPS having state-of-the-art security measures integrated, thereby increasing the level of protection even further.

VI. CONCLUSION

A CPS comprises cyber-technology and the physical world. Both parts have to be covered by a security concept and solution. Traditional cyber security puts the focus on the cyber-part, i.e., automation and control systems. The security of the physical part, like machinery, is protected often by physical and organizational security measures, only. This paper presented the concept for a new approach that enhances the achieved level of security by protecting the interface between the cyber-part and the physical world, thereby enhancing the resilience of a CPS being under attack.

 ISBN: 978-1-61208-743-6

REFERENCES

[1] P. England, R. Aigner, A. Marochko, D. Mattoon, R. Spiger, S. Thom, "Cyber resilient platforms", Microsoft Technical Report MSR-TR-2017-40, Sep. 2017, available from: https://www.microsoft.com/en-us/research/publication/cyber-resilient-platforms-overview/ 2019.07.19

[2] Electronic Communications Resilience&Response Group, "EC-RRG resilience guidelines for providers of critical national telecommunications infrastructure", version 0.7, March 2008, available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62281/telecoms-ecrrg-resilience-guidelines.pdf 2019.07.19

[3] D. Urbina, J. Giraldo, N. O. Tippenhauer, A. Cardenas, "Attacking fieldbus communications in ICS: applications to the SWaT testbed", Singapore Cyber-Security Conference (SG-CRC), IOS press, pp. 75–89, 2016, available from: http://ebooks.iospress.nl/volumearticle/42054 2019.07.19

[4] C. C. Davidson, T. R. Andel, M. Yampolskiy, J. T. McDonald, W. B. Glisson, T. Thomas, "On SCADA PLC and fieldbus cyber security", 13th International Conference on Cyber Warfare and Security, National Defense University, Washington, DC, pp. 140–148, 2018

[5] D. Bodeau and R. Graubart, "Cyber resiliency design principles", MITRE Technical Report, January 2017, available from: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf 2019.07.19

[6] R. Falk and S. Fries, "Enhancing integrity protection for industrial cyber physical systems", The Second International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2017, pp. 35–40, November 12 - 16, 2017, Barcelona, Spain, available from: http://www.thinkmind.org/index.php?view=article&articleid=cyber_2017_3_30_80031 2019.07.19

[7] European Commission, "The directive on security of network and information systems (NIS Directive)", available from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive 2019.07.19

[8] IEC 62443, "Industrial automation and control system security" (formerly ISA99), available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx 2019.07.19

[9] ISO/IEC 27001, "Information technology – security techniques – Information security management systems – requirements", October 2013, available from: https://www.iso.org/standard/54534.html 2019.07.19

[10] IEC 62443-3-3:2013, "Industrial communication networks – network and system security – Part 3-3: System security requirements and security levels", Edition 1.0, August 2013

[11] IEC 62554-4.2, "Industrial communication networks - security for industrial automation and control systems - Part 4-2: technical security requirements for IACS components", CDV:2017-05, May 2017

[12] P. Bock, J.-P. Hauet, R. Françoise, R. Foley, "Ukrainian power grids cyberattack - A forensic analysis based on ISA/IEC 62443", ISA InTech magazine, 2017, https://www.isa.org/templates/news-detail.aspx?id=152995 2019.07.19

[13] ZVEI, „Orientation guideline for manufacturers on IEC 62443", "Orientierungsleitfaden für Hersteller zur IEC 62443" [German], ZVEI Whitepaper, 2017, https://www.zvei.org/presse-medien/publikationen/orientierungsleitfaden-fuer-hersteller-zur-iec-62443/ 2019.07.19

[14] T. Hupperich, H. Hosseini, T. Holz, "Leveraging sensor fingerprinting for mobile device authentication", International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, LNCS 9721, Springer, pp. 377–396, 2016, available from: https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2016/09/28/paper.pdf 2019.07.19

[15] H. Bojinov, D. Boneh, Y. Michalevsky, G. Nakibly, "Mobile device identification via sensor fingerprinting", arXiv:1408.1416, 2016, available from: https://arxiv.org/abs/1408.1416 2019.07.19

[16] P. Hao, "Wireless device authentication techniques using physical-layer device fingerprint", PhD thesis, University of Western Ontario, Electronic Thesis and Dissertation Repository, 3440, 2015, available from: https://ir.lib.uwo.ca/etd/3440 2019.07.19

 ISBN: 978-1-61208-743-6