Enhancing Attack Resilience in the Presence of Manipulated IoT Devices within a Cyber Physical System

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

***Abstract*—Industrial cyber physical systems are exposed to attacks. Security standards define how such systems and the used devices can be protected against attacks (prevent). Despite all efforts to protect from attacks, it should always be assumed that attacks may happen. Security monitoring allows to detect successful attacks (detect), so that corresponding measures can be performed (react). This prevent-detect-react cycle is common approach in security of information technology and operation technology. This paper describes an additional approach for protecting cyber physical systems. The devices are designed in a way that makes it harder to use them for launching attacks on other devices. A device-internal hardware-based or isolated firewall limits the network traffic that the device software executed on the device can send or receive. Even if the device software contains a vulnerability allowing an attacker to compromise the device, the possible impact on other connected devices is limited, thereby enhancing the resilience of the cyber physical system in the presence of manipulated devices.**

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

I. INTRODUCTION

Traditionally, IT security has been focusing on information security, protecting confidentiality, integrity, and availability of data at rest and data in transit, and sometimes also protecting data in use by confidential computation. 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, intelligent traffic management, and power system management. Cyber security is covering different phases during operation as there are protect, detect, and react: Protecting against threats, detecting when an attack has occurred, and recovering from attacks.

When designing a security solution for a CPS or a device used within the CPS, the focus is on protecting the assets of the CPS or device, by preventing attacks against the relevant assets. However, this is not sufficient from a more holistic perspective: Also, the environment of a device or a CPS has to be protected from attacks originating from a manipulated CPS or one of its devices. In particular, Internet of Things (IoT) devices have been attacked with the objective to use them for launching attacks against *other* systems. Dao, Phan et al. described distributed denial of service (DDoS) attacks originating from manipulated IoT devices [1]. As (consumer) IoT devices have often also a weak security management, so that vulnerabilities are often not patched in time, making them an easy victim.

This paper presents an approach for protecting the network environment, i.e., other devices of a CPS and further connect devices, from attacks originating from a manipulated component of the CPS. The objective is to limit the impact of a manipulated CPS device on other devices of the CPS, enhancing resilience of the CPS. The intention is to keep the CPS in an operational state even if some devices of the CPS should have been successfully attacked and be manipulated. Devices have to be designed in a way that it is made hard to use them for attacks even if they should be hacked. After giving an overview on cyber physical systems and on industrial cyber security in Sections II and III, a new approach on protecting the network environment from manipulated devices of a CPS 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 (IACS), monitors and controls a technical system. Examples are process automation, machine control, energy automation, and cloud robotics. Automation control equipment with sensors (S) and actuators (A) is 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 by determining the corresponding actuator signals.

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,

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-893-8

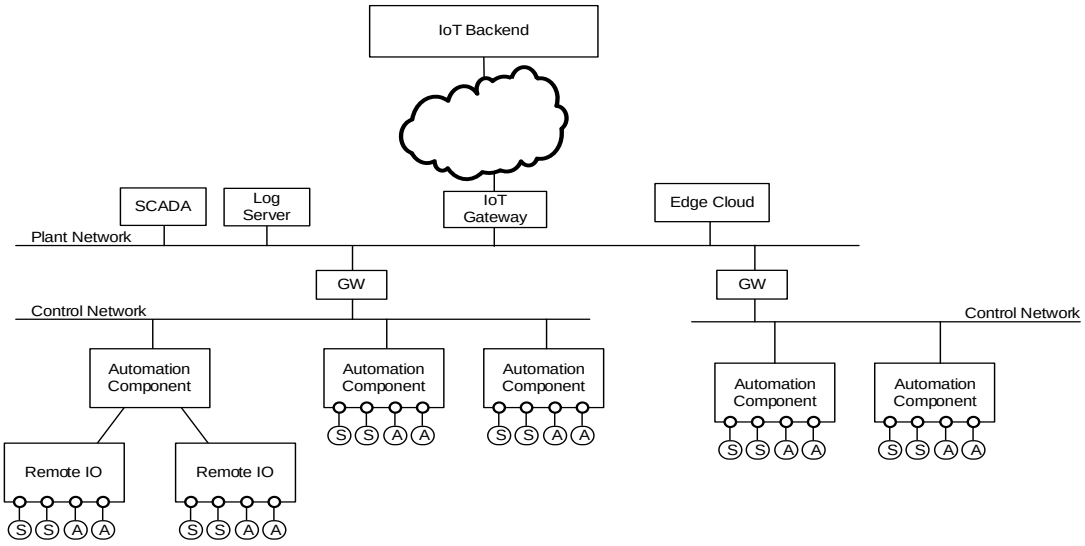

Figure 1. Example – Industrial Automation and Control System

or to enforce a specific security policy within a production cell. Such an industrial automation and control system is an example of a CPS and is utilized in various automation domains, including discrete automation (factory automation), process automation, railway automation, energy automation, and building automation.

Figure 2 shows the typical simplified 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.

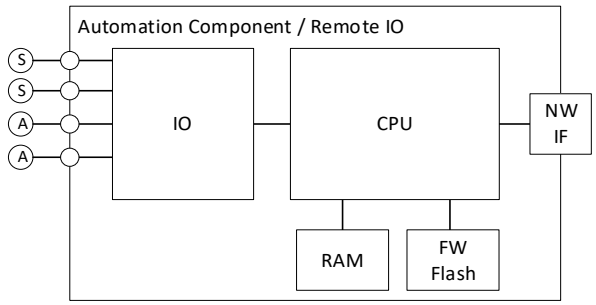

Figure 2. Automation Component

In practice, it has to be assumed that each software component may comprise vulnerabilities, independent of the effort spend to ensure high software quality. This is one reason why automation systems are usually organized in separate security zones. Network traffic can be filtered using network firewalls between different zones, limiting the impact of an impact in one security zone on other connected security zones. In addition, it is often not possible to fix known vulnerabilities immediately by installing a software update, as updates have to be tested thoroughly in a test system before being installed in an operational system, and as an installation is often possible only during a scheduled maintenance window. Also, the priorities of security objectives in different security zones are often different, too. In CPSs, the impact of a vulnerability in an OT system may not only affect data and data processing as in classical IT, but it may have an effect also on the physical world. For example, production equipment could be damaged, or the physical process may operate outside the designed physical boundaries, so that the produced goods may not have the expected quality or even that human health or life is endangered.

III. INDUSTRIAL CYBER SECURITY

Protecting IACSs 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 [11].

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 preventing the direct application of security concepts established in the IT domain 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.

The three basic security requirements are confidentiality, integrity, and availability (“CIA” requirements). However, in automation systems or industrial IT, the priorities are commonly just the other way around: Availability of the IACS has typically the highest priority, followed by integrity. Confidentiality is often no strong requirement for control communications, but may be needed to protect critical business know-how.

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-893-8

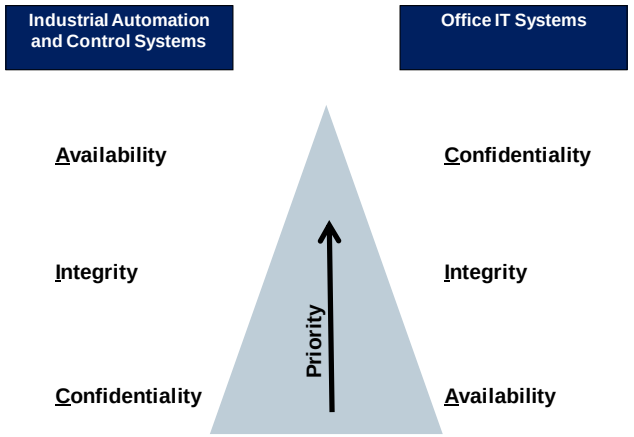

Figure 3. The CIA Pyramid [9]

Figure 3 shows that in common IT systems, the priority is "CIA". As shown graphically, the CIA pyramid is inverted (turned upside down) in many automation systems.

Specific requirements and side conditions of an IACS 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 cyber security solution. Often, an important aspect is that the applied security measures do not put availability and integrity of the automation system at risk. 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 [10] 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 framework IEC 62443 [11] 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. Specific parts of this framework are applied successfully in different automation 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 for the industrial domain 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 27001 [12] or the NIST cyber security framework. 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.

Different parts of the IEC62443 standard are grouped into four clusters, covering:

- common definitions and metrics;
- requirements on setup of a security organization (ISMS related, similar to ISO 27001 [12]), as well as solution supplier and service provider processes;
- technical requirements and methodology for security on system-wide level, and
- requirements on the secure development lifecycle of system components, and security requirements to such components at a technical level.

The framework parts address different roles over different phases of the system lifecycle: The operator of an IACS operates the IACS that has been integrated by the system integrator, using components of product suppliers. In the set of corresponding documents, security requirements are defined, which target the solution operator and the integrator but also the product manufacturer.

According to the methodology described in IEC 62443 part 3-2, a complex automation system is structured into zones that are connected by and communicate through so-called "conduits" that map for example to the logical network protocol communication between two zones. Moreover, this document defines Security Levels (SL) that correspond with the strength of a potential adversary. To achieve a dedicated SL, the defined requirements have to be fulfilled.

Part 3-3 of IEC 62443 [14], addressing an overall automation system, is in particular relevant for the system integrator. It defines seven foundational requirements that 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, several concrete technical security requirements (SR) and requirement enhancements (RE) are defined. Related security requirements are defined for the components of an industrial automation and control system in IEC 62443 part 4-2 [15], addressing in particular component manufacturers.

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-893-8

IV. PROTECTING NETWORK ENVIRONMENT FROM MANIPULATED IOT DEVICES

The security objective "resilience under attack" means that a CPS, e.g., an IACS or an industrial Internet of Things (IoT) environment, should stay operational even when some devices would be manipulated. Considering the manifold of devices used in real-world CPS, it has to be assumed that some of them will have vulnerabilities that can be used to install malware to attack other devices. Hence, it shall be avoided that a successfully hacked device can be used to launch attacks against other devices. This is a specific security objective: When designing the security architecture for a device, usually attacks against the device are investigated. Here, it shall be avoided that even if a device would be attacked successfully despite its designed-in protection means, the impact of this attack on the network environment is reduced.

The software execution environment executes the software (firmware) of the device that might have a vulnerability. A separated, e.g., a separate hardware based, on-device firewall limits the network communication that the executed software can perform. This enforcement is realized independently from the executed device software, so that it is still working even if the device software has been manipulated by an attacker. This independence is a necessary pre-requisite. In the described design, this independence is achieved by separate hardware-based component. However, the independence from the executed device software could be achieved also by using an isolated software execution environment, e.g., a separate processor or a separate trusted execution environment. Using a hardware-based realization has the advantage of limiting the impact on real-time communication properties as delay and jitter, and also on the energy consumption. It can be easily implemented if a dedicated hardware-based network interface is in use anyhow to support real-time communication protocols.

Possible filter criteria are source and destination network addresses, protocols, port numbers, transmit rate (frames/packets per second), or data volume. In an advanced form, the firewall may even verify on application level, whether certain control flows are aligned with either the typical (historical) behavior of the device or with an engineered process. The policy might be fixed, e.g., for embedded control devices with a fixed functionality, or configurable. Important is that the device software cannot modify the filter policy on its own.

The filter policy might be adapted automatically depending on the patch status of the device software, or depending on a cryptographically protected health check confirmation received from a device integrity monitoring service. This would allow to keep the system operational, although with potentially limited capabilities, thus keeping it resilient. Also, limiting specific functionalities as result of missing device integrity may stipulate the timely application of patches, to get the system back to normal operation with full functionality and performance.

Figure 4 shows an IoT Field Device with a central processing unit CPU executing device firmware/software stored in a flash of RAM memory.

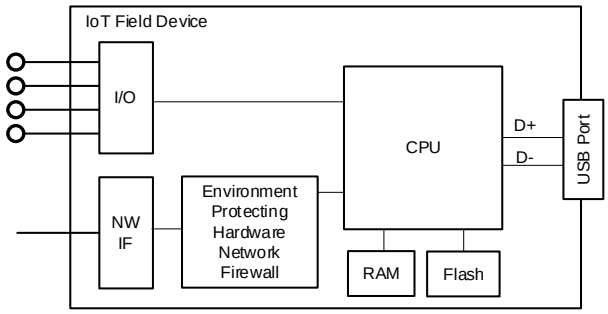

Figure 4. Attack-preventing IoT Device Architecture

The software can communicate over the network interface (NW IF) with other devices, e.g., using HTTPS or OPC UA over TCP/IP. Also, sensors and actuators can be connected via an input-output (I/O) interface. An USB interface allows to configure the device or to install a firmware update.

To enhance resilience, the device includes a hardware-based network firewall to protect the network environment from attacks originating from the IoT field device. It limits the type of network communication that can be performed by the device software executed on the CPU. This function is fixed, so that the device software cannot modify it, so that the filtering is performed with high level of trustworthiness. The hardware-based network firewall is still effective even if the device software should be manipulated.

The hardware-based firewall can be realized by an integrated circuit, e.g., an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA), or a separate microcontroller or security controller, or it can be integrated with a hardware-based network interface. The filter policy might be adapted, depending on whether a cryptographically protected network access token (NAcT) is provided to the hardware firewall. The NAcT can be provided by a backend device integrity check service. The device software may provide a received NAcT token to the device hardware firewall, but cannot manipulate it. This allows the backend device integrity check service to temporarily activate a less restrictive policy if the device integrity has been verified successfully. A NAcT token can be protected by a cryptographic checksum, e.g., a digital signature (e.g., RSA, DSA, ECDSA) or a symmetric message authentication code (e.g., HMAC, AES-CBC-MAC). The NAcT token realizes an authenticated watchdog, as described by England, Aigner, Marochko, Mattoon, Spiger, and Thom [3]. However, here it is used for selecting a firewall policy, not for initiation a device recovery procedure. If an integrity monitoring system monitoring the integrity of control devices or a network-based intrusion detection system, realizing the device integrity check service, detects an ongoing attack in the IACS, it can limit reliably the network communications of devices, allowing to confine the attack.

A different approach compared to attack monitoring is to monitor write access to the flash memory, i.e., to check whether the device software (firmware) stored in the flash memory is updated regularly. The less restrictive, open filter policy stays activated only if the device firmware is updated regularly.

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-893-8

V. EVALUATION

While the original motivation for ”plug and produce”, as defined for Industry 4.0, is to increase flexibility in production and to reduce the time needed to reconfigure an automation environment for different manufacturing tasks or batches, this flexibility is also advantageous for increasing resilience under attack: Even if some of the devices are manipulated (attacked) and cannot be used for production until they are patched, the flexibility of the overall production system allows to reconfigure the IACS components, avoiding or at least limiting the interaction with affected devices. Therefore, production can continue, maybe with limitations, even when some devices should have been manipulated. When using the enhancement described in section IV, it depends on the specific IACS and on the specific attack scenario to what degree the IACS can stay operational under attack. For the evaluation, it has to be determined to what degree relevant risks of the IACS are reduced by introducing such protection measures.

The security of a CPS is evaluated in practice in various approaches and stages of the system’s lifecycle:

- A Threat and Risk Analysis (TRA, also abbreviated as TARA) is typically conducted at the beginning of the product or system development, and updated after major design changes, or to address a changed threat landscape. In a TRA, possible attacks (threats) on the system are identified. The impact that would be caused by a successful attack and the probability that the attack happens are evaluated to determine the risk of the identified threats. The risk evaluation allows to prioritize the threats, focusing on the most relevant risks and to define corresponding security measures. Security measures can target to reduce the probability of an attack by preventing it, or by reducing the impact.
- Security checks can be performed during operation or during maintenance windows to determine key performance indicators (e.g., check compliance of device configurations) and to verified that the defined security measures are in fact in place.
- Security testing (penetration testing, also called pentesting for short) can be performed for a system that has been built, but that is currently not in operation. A pentest can usually not be performed on an operational automation and control system, as the pentest could endanger the reliable operation auf the system. Pentesting can be performed during a maintenance window when the physical system is in a safe state, or using a separate test system. Security testing can be performed also on a digital representation of a target system, e.g., a simulation in the easiest case. This digital representation is also called “digital twin”. This allows to perform security checks and pentesting for systems that are not existing yet physically (design phase), or to perform pentesting of operational systems in the digital world without the risk of disturbing the regular operation of the real-world system.

As long as the technology proposed in the paper has not been proven in a real-world operational setting, it can be evaluated conceptually by analyzing the impact that the additional security measure would have on the identified residual risks as determined by a TRA. The general effect of the presented security measure is that the impact of a threat, i.e., a successful attack, on the physical world controlled by the CPS is reduced. Whatever attack is ongoing on the IT-based automation and control system, still the possible impact on the real, physical world is limited. While security measures often target the prevention of attacks, the proposed resilience measure reduces the impact and thereby the risk. The impact of a threat is reduced if the IACS in fact can stay operational, at least with limited functionality, in relevant attack scenarios.

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 of the chemicals / consumables 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. Both, the trusted sensors and the physical world firewall build a security overlay network, independent from the actual operational control network. Thereby, a physical damage of the production equipment can be avoided. If needed, a controlled shutdown of the production site can be performed.

As the evaluation in a real-world CPS requires significant effort, and as attack scenarios cannot be tested that could really have a (severe) impact on the physical world, a simulation-based approach or using specific test-beds are possible approaches, allowing to simulate or evaluate in a protected test-bed the effect on the physical world of certain attack scenarios with compromised components. The simulation would have to include not only the IT-based control function, but also the physical world impact of an attack. Using physical-world simulation and test beds to evaluate the impact of attacks have been described by Urbina, Giraldo et al. [24].

VI. CONCLUSION

A CPS comprises the operational cyber-technology and the physical world with which the system interacts. 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 a concept for a new approach that enhances the resilience of a CPS in the presence of attacked devices, by making it harder that a compromised device is used for attacking other devices of the CPS. This can be a useful element to ensure the availability of the automation system, as even under attack, the automation system has not to be shut down. It is complementary to other approaches for enhancing CPS resilience by protecting the physical-world interface [2].

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-893-8

REFERENCES

[1] N. N. Dao, T. V. Phan, Umar Sa'ad, Joongheon Kim, Thomas Bauschert, and Sungrae Cho, "Securing Heterogeneous IoT with Intelligent DDoS Attack Behavior Learning", arXiv: 1711.06041v3 [cs.NI] 7 Aug 2019, [Online]. Available from: https://arxiv.org/pdf/1711.06041.pdf [retrieved August, 2021]

[2] R. Falk and S. Fries, "Enhancing Resilience by Protecting the Physical-World Interface of Cyber-Physical Systems", The Fourth International Conference on Cyber-Technologies and Cyber-Systems CYBER 2019, pp. 6–11, September 22, 2019 to September 26, 2019 - Porto, Portugal, [Online]. Available from: https://www.thinkmind.org/index.php?view=article&articleid=cyber_2019_1_20_80033 [retrieved August, 2021]

[3] P. England, R. Aigner, A. Marochko, D. Mattoon, R. Spiger, and S. Thom, "Cyber resilient platforms", Microsoft Technical Report MSR-TR-2017-40, Sep. 2017, [Online]. Available from: https://www.microsoft.com/en-us/research/publication/cyber-resilient-platforms-overview/ [retrieved August, 2021]

[4] 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 [retrieved August, 2021]

[5] D. Urbina, J. Giraldo, N. O. Tippenhauer, and A. Cardenas, "Attacking fieldbus communications in ICS: applications to the SWaT testbed", Singapore Cyber-Security Conference (SG-CRC), IOS press, pp. 75–89, 2016, [Online]. Available from: http://ebooks.iospress.nl/volumearticle/42054 [retrieved August, 2021]

[6] C. C. Davidson, T. R. Andel, M. Yampolskiy, J. T. McDonald, W. B. Glisson, and 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

[7] D. Bodeau and R. Graubart, "Cyber resiliency design principles", MITRE Technical Report, January 2017, [Online]. Available from: https://www.mitre.org/sites/default/files/publications/PR%20170103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf [retrieved August, 2021]

[8] A. Kott and I. Linkov (Eds.), "Cyber Resilience of Systems and Networks", Springer, 2019

[9] 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, [Online]. Available from: http://www.thinkmind.org/index.php?view=article&articleid=cyber_2017_3_30_80031 [retrieved August, 2021]

[10] European Commission, "The directive on security of network and information systems (NIS Directive)", [Online]. Available from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [retrieved August, 2021]

[11] IEC 62443, "Industrial automation and control system security" (formerly ISA99), [Online]. Available from: https://webstore.iec.ch/searchform&q=62443 [retrieved August, 2021]

[12] ISO/IEC 27001, "Information technology – security techniques – Information security management systems – requirements", October 2013, [Online]. Available from: https://www.iso.org/standard/54534.html [retrieved August, 2021]

[13] NIST, "Framework for Improving Critical Infrastructure Cybersecurity", Version 1.1, April 16, 2018, [Online]. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [retrieved August, 2021]

[14] 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

[15] IEC 62443-4.2, "Industrial communication networks - security for industrial automation and control systems - Part 4-2: technical security requirements for IACS components", Feb. 2019

[16] P. Bock, J. P. Hauet, R. Françoise, and R. Foley, "Ukrainian power grids cyberattack - A forensic analysis based on ISA/IEC 62443", ISA InTech magazine, 2017, [Online]. Available from: https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack [retrieved August, 2021]

[17] ZVEI, "Orientation guideline for manufacturers on IEC 62443", "Orientierungsleitfaden für Hersteller zur IEC 62443" [German], ZVEI Whitepaper, 2017, [Online]. Available from: https://www.zvei.org/presse-medien/publikationen/orientierungsleitfaden-fuer-hersteller-zur-iec-62443/ [retrieved August, 2021]

[18] H. R. Ghaeini, M. Chan, R. Bahmani, F. Brasser, L. Garcia, J. Zhou, A. R. Sadeghi, N. O. Tippenhauer, and S. Zonouz, "PAtt: Physics-based Attestation of Control Systems", 22nd International Symposium on Research in Attacks, Intrusions and Defenses, USENIX, pp. 165–180, September 23-25, 2019, [Online]. Available from: https://www.usenix.org/system/files/raid2019-ghaeini.pdf [retrieved August, 2021]

[19] Plattform Industrie 4.0, "Industrie 4.0 Plug-and-produce for adaptable factories: example use case definition, models, and implementation", Plattform Industrie 4.0 working paper, June 2017, [Online]. Available from:https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/Juni/Industrie_4.0_Plug_and_produce/Industrie-4.0-_Plug-and-Produce-zvei.pdf [retrieved August, 2021]

[20] T. Hupperich, H. Hosseini, and 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, [Online]. Available from: https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2016/09/28/paper.pdf [retrieved August, 2021]

[21] H. Bojinov, D. Boneh, Y. Michalevsky, and G. Nakibly, "Mobile device identification via sensor fingerprinting", arXiv:1408.1416, 2016, [Online]. Available from: https://arxiv.org/abs/1408.1416 [retrieved August, 2021]

[22] P. Hao, "Wireless device authentication techniques using physical-layer device fingerprint", PhD thesis, University of Western Ontario, Electronic Thesis and Dissertation Repository, 3440, 2015, [Online]. Available from: https://ir.lib.uwo.ca/etd/3440 [retrieved August, 2021]

[23] R. Falk and M. Trommer, "Integrated Management of Network and Host Based Security Mechanisms", 3rd Australasian Conference on Information Security and Privacy, ACISP98, pp. 36-47, July 13-15, 1998, LNCS 1438, Springer, 1998

[24] D. Urbina, J. Giraldo, A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting The Impact of Stealthy Attacks on Industrial Control Systems", ACM Conference on Computer and Communications Security (CCS), pp. 1092–1105, Vienna, Austria, 2016