Security Challenges and Best Practices for IIoT

Edita Bajramovic[1], Deeksha Gupta[2], Yun Guo[3], Karl Waedt[4], Anis Bajramovic[5]

Abstract: Security concerns regarding the Industrial Internet of Things (IIoT) are constantly increasing, causing issues in industrial facilities, where heavy machinery and dangerous systems are operated and controlled with connected devices. Some of the recent security incidents e.g. Stuxnet worm (Advanced Persistent Threat) and theft of sensitive information in South Korea Nuclear Power Plant (Insider Threat) have shown that these attacks should be considered as the top threat to IIoT, including nuclear facilities. Yet, as industrial systems become more and more interconnected, comparable cyber-attacks could happen in other industrial domains in the future. Therefore, adequate international standards and best practices can decrease occurrence of such attacks.

Keywords: IIoT; Security; Standards; Best Practices

1 Introduction

The main goal of an Industrial Internet of Things (IIoT) system is to connect and incorporate industrial control systems with enterprise systems, business processes and analytics. An IIoT system provides considerable improvements in enhancing decision-making, operations and relationships between many independent control systems. Hence, these systems are very different from traditional industrial control systems and traditional information technology (IT) systems [Sc16]. Such IIoT systems are connected to other systems and people, using sensors and actuators in an industrial setting. Furthermore, IIoT systems are interconnected with the physical domain where any type of uncontrolled or intentional or unintentional modification can cause dangerous incidents. This apparent risk intensifies the significance of safety, reliability, privacy and resiliency past the anticipated levels in various traditional IT settings. As these systems have long lifecycles and consist of many legacy systems, they have to be maximally regulated. All of above mentioned different aspects suggest that IIoT systems must be adequately secured.

1.1 Contribution

The aim of this paper is to describe some of the security challenges and best practices in IIoT. To summarize, we provide following contributions in this paper:

[1] Friedrich Alexander University Erlangen-Nuremberg, Department of Computer Science, Martensstrasse, 91058 Erlangen, Germany, edita.bajramovic@fau.de
[2] Framatome GmbH, Henri-Dunant-Strasse 50, 91058, Erlangen, Germany, deeksha.gupta@framatome.com
[3] Huaneng Shandong Shidao Bay Nuclear Power Co..LTD, No.9 Shihe Road, Rongcheng, Shandong Province, China, guoyun_2018@163.com
[4] Framatome GmbH, Henri-Dunant-Strasse 50, 91058, Erlangen, Germany, karl.waedt@framatome.com
[5] University of Maryland University College, MD, USA, anisba@gmail.com

doi:10.18420/inf2019_ws28

1. We review several well-known standards related to security of IIoT in different domains, including newly developed IEC 63096 standard. We briefly provide main focus of each standard. Furthermore, we discuss RAMI 4.0 platform.
2. We survey security challenges, outline major risks and mention some of the most recent cyber attacks.
3. Based on surveyed security challenges, we provide security recommendation for best practices in IIoT.

Development and progress of Industry 4.0 is guided by the "German Standardization Roadmap Industrie 4.0"[Ge18]. Currently, this is available as version 3 while version 4 is being prepared. Despite its length of almost 150 pages, the security part is quite high-level. The SSecurity Standards White Paper for Sino-German Industrie 4.0/ Intelligent Manufacturing"provides some further guidance, including on the application of specialized IT security standards for the Industry 4.0 and IIoT world [Al].

Our paper provides further guidance based on experience from past projects, which also consider further Industry 4.0 concepts like Automation ML and OPC UA. As OPC UA and Time Sensitive Networks (TSN) form the basis of the Industry 4.0 interoperability, the respective security concepts from ISO/IEC 62541-2 [IEC02] are also considered.

Our recommendations are at the concepts and architecture level. We will provide further guidance in other publications, e.g. on the implementation of Attribute Based Access Control for IIoT, the use of FPGAs, mixed criticality systems, for efficiently putting into practice IEC 62443-3-3 [IEC13] concepts.

1.2 Paper Outline

We first present several well-known standards applied in securing IIoT in Section 2. We then introduce Reference Architecture Model of Industry 4.0 in Section 3. In Section 4, we perform survey of security challenges in IIoT. Section 5 outlines some of the most recent cybersecurity incidents. Lastly, in Section 6 we recommend best practices to be applied in IIoT.

2 International Standards

Many standards and regulations, associated with the protection of IIoT systems, are published by standards organizations and regulatory body. Here, we give short overview of standards that are related generally to IIoT systems.

2.1 IEC 62443

Entire series of IEC 62443 [IEC13, IEC15] standards for industrial automation and controls systems security are published by the International Electrotechnical Commission (IEC). The idea of these series is to provide guidelines regarding manufacturing and control

systems security, dealing with various categories of systems, facilities, and plants in different industries [Sc16]. Currently, IEC 62443 series of standards contains four different parts. Part 1 (IEC 62443-1-1 [IEC09]) introduces terms and definitions and provides reliable models, references and metrics indicated in other parts. Part 2 (IEC 62443-2-1 [IE10], IEC 62443-2-2 [IE18a], IEC 62443-2-3 [IE15]) discusses policies and procedures used to generate efficient security programs for Industrial Control Systems (ICS). Furthermore, Part 3 (IEC 62443-3-1 [IE09], IEC 62443-3-3 [IEC13]) contains information regarding security technologies, security requirements and security levels in Industrial Control Systems (ICS). Lastly, Part 4 (IEC 62443-4-1 [IE18b], IEC 62443-4-2 [IEC15]) covers requirements for secure development lifecycle for ICS and security requirements for control system components.

2.2 NIST 800-82

NIST SP 800-82 [St15] provides guidance on enhancing security in ICS. This standard also focuses on Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs) and etc. Furthermore, security controls outlined in this standard are also mapped to NIST SP 800-53 [NI13] and NIST SP 800-183 [Vo16].

2.3 NERC CIP

North American Electric Reliability Corporation (NERC) also published standards for Critical Infrastructure Protection (CIP) [NER19]. These standards describe auditable requirements for CIP in order to enhance the security of the electric industry. Their focus is on automation systems integrated in generation and transmission facilities.

2.4 IEEE 1686

All aspects of Intelligent Electronic Devices (IEDs) are described in the IEEE 1686 standard for Intelligent Electronic Devices Cybersecurity [IEE13]. This standard defines requirements for IED access, configuration, operation, etc.

2.5 IEC 63096

For I&C systems in nuclear power plants, IEC 63096 [BQB17] focuses on in detail the selection and application of computer security controls from the included security controls catalogue. The main goal is to prevent, detect and react to digital attacks against computer-based I&C systems using graded approach. This standard applies to instrumentation & control of new nuclear power plants and to the I&C modernization in existing plants.

3 RAMI 4.0

The Reference Architecture Model of Industry 4.0 [HR15](RAMI 4.0) provides an integrated approach for the comprehensive coverage of the Industry 4.0 targets. The 3-dimensional structure, as indicated in Figure 1 contains 3 axis:

- The “Hierarchy Levels” axis
- The “Lifecycle and Value stream” axis
- The “Layers” axis

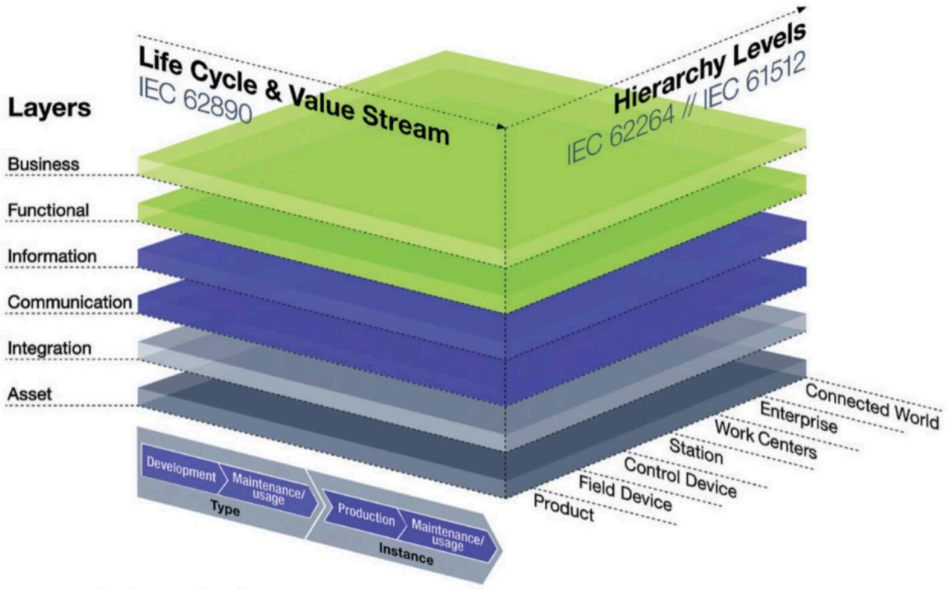

Fig. 1: RAMI 4.0 [Al]

The “Hierarchy Levels” (bottom, horizontal right) are named according to the enterprise IT and control systems addressed by IEC 62264 [IE02]. These start with an individual “Product” connected to a “Field Device” that is managed by a “Control Device”. The “Control Device” is part of a “Station” controlled by a “Work Center” of an “Enterprise”. The connected enterprises are named “Connected World”.

Along the “Lifecycle” (bottom, horizontal left) axis there are two parts:

- The “Development” and maintenance of products and platforms
- The “Production” (at a factory) or the operation (of a plant)

The “Development” part of the “Lifecycle” explicitly considers the maintenance at the product and platform level. The development of products results in “Type” tested samples (typicals), that may even require certification, for safety critical applications.

The “Production” part of the “Lifecycle” also explicitly contains a maintenance sub-phase. This is at the “Instance” level. Each manufactured entity of a typical is an “Instance”. The maintenance of the instance is different from the maintenance of a typical. The “Instance” may be a specific manufacturing robot, that needs a re-calibration after a given number of operation hours [Al].

The six layers along the vertical “Layers” axis describe a layered break-down according to the properties of complex systems. At the bottom the “Assets” are integrated (“Integration”).

The “Information” collected via the “Communication” layer is provided as a “Functional” layer and a “Business” layer”. Addressing the functional safety and cybersecurity in the context of the RAMI 4.0 (and Intelligent Manufacturing System Architecture (IMSA) model in China) are ongoing topics. In principle this has to be done for each of the small cubes resulting from intersections at a given point in the RAMI cube [Al]. For example a “Field Device” [“Hierarchy Levels” 2] may be considered as an “Asset” [“Layers” 1]

- during the device “Development” phase [“Lifecycle” 1], e.g. by secure development guidelines,
- during the device “Type” maintenance, e.g. by correcting the firmware,
- during the device “Production”, by securing the production environment of each “Instance”
- during the device “Instance” maintenance, e.g. by disabling some users, that should no longer have access to the instance.

These for examples correspond to 4 small cubes out of the total of 7x4x6 (in RAMI, and slightly different number in IMSA).

The above example shows that the RAMI 4.0 model derived from real world challenges. It is also based on already well established standards and well understood lifecycle phases along each of the 3 axis [Ge18].

4 Security Challenges

Even with many advantages of accepting Industry 4.0 technologies and making critical infrastructure “Smart”, security challenges are present. According to the Kaspersky Lab’s The State of Industrial Cybersecurity 2018 report [SP18], 65% of companies consider higher probability of cybersecurity risks for OT/ICS with implementation IIoT technologies. Therefore, industries face many security challenges and we will just briefly describe a few of them.

4.1 Vulnerable Components

The Industrial Internet of Things (IIoT) landscape is emerging rapidly. Millions of devices are connected worldwide, thus urging to adequately secure IIoT in critical infrastructure

[Go18]. Most existing components were not developed with concept of security-by-design in mind, posing great challenge to industrial environments. Vulnerabilities in such systems are attractive target to cyber attackers. Hence, components in IIoT are not an isolated concept. They are jointly connected with many security disciplines such as IT security, OT security and physical safety. Change from totally closed to open connected cyber physical systems enforce appropriate handling the vulnerabilities in such systems [Go18].

4.2 Increased Interconnectivity

Industrialized processes require collaboration with entities and environments on a global level and systems used in critical infrastructure, leading to joint cooperation between many organizations. One of the major challenges for greater connectivity is that security can have a serious impact on safety [Go18].

4.3 IT/OT Merging

ICSs gradually stopped to be isolated after the merging of IT devices in the ICS sphere become a common practice. Merging with IT network-enabled groups allowed for simplification and handling of sophisticated environments while also bring together new cybersecurity risks. Major challenge is to find appropriate ways to handle IT/OT incorporation [Go18]. Significant aspects include unprotected network connections, deployment of technologies with identified vulnerabilities that bring together formerly unidentified risks into the OT environment, and inadequate perception of requirements for ICS settings. Holistic security must protect digital and physical operation [Go18].

4.4 Legacy Systems

According to World Economic Forum Report [OK15], legacy systems are a major obstacle towards implementation of the Industrial Internet of Things. Companies tend to create new innovative systems on top of legacy systems, resulting in obsolete protection measures and comprise undiscovered vulnerabilities that have been idle for some time. Implementing new IIoT devices to old-fashioned and outdated hardware brings new threats that permit attackers to discover new ways to attack systems.

4.5 Human Factors

Accepting new technologies and know-how causes that production workers, office employees, and engineers have to work with new categories of information, networks and systems using innovative techniques. They are usually unaware of the security risks related to collecting, managing and evaluating such information. As a result, they may become victims of cyber attackers. According to NTT Security 2017 Global Threat Report [NTT17], 73 % of malware attacks started with phishing emails. This is very disturbing and showing that the people are weakest link in the security.

5 Security Incidents

In recent years, many cybersecurity incidents occurred in critical infrastructure. Here, we provide four cybersecurity incidents that occurred in Industry 4.0.

5.1 WannaCry Ransomware Global Cyber-Attack

This massive cyber-attack affected more than 230,000 computers in 150 countries. The target were among others manufacturers, banks and governments worldwide. While many companies e.g. Renault and Honda had to stop the production, FedEx customers had late deliveries [Go18]. Furthermore, in the UK, National Health Service had to terminate all meeting arrangements. Those are only examples of a small number of victims who confirmed that they were target of this ransomware. Many other companies did not want to confirm that they were infected with WannaCry. WannaCry is virus that uses two complex exploits in Microsoft Windows systems. This virus is spread through the Server Message Block (SMB) protocol [Go18]. It installs itself on a vulnerable machine and does not require any user action. Once it gained access, the virus infects other targets and spreads further. However, this virus contained a flaw that permitted researchers to slow down the attack, allowing asset owners short time to protect their vulnerable devices. If the security updates were installed a few months earlier, the devices would be adequately secured from this attack [Go18].

5.2 Industroyer Second Cyberattack on Ukrainian Power Grid

This second cyber-attack on the Ukrainian power grid has many similarities with the first cyber-attack that occurred one year before. The only difference of two attacks was the used method of the attack. For the second attack, a new special malware was developed to target electrical grids and it was called Industroyer. The main targets of this malware were communication protocols, allowing the cyber-attacker to gain access to an industrial control system using backdoor and opening circuit breakers to stop power supply. The attackers deleted important files, causing systems to stop responding. There are implications that Industroyer can be altered to attack other types of critical infrastructure, posing a major threat to ICS [Go18, CL17].

5.3 German Steel Mill Attack

German steel mill attack has started with a phishing email opened by careless employee. Once entered into network, by still unknown techniques, attackers gained access to plant network and took control of many ICS devices, e.g. PLCs, HMIs, and alarm systems [Go18]. Afterwards, attackers manipulated some particular systems and cause system failure. They also interrupted safe shutdown of a blast furnace and caused severe physical destruction to the system.

5.4 Venezuela Blackout

On March 7th, more than 20 of Venezuela's 23 states, including the capital, Caracas, lost power for more than 24 hours, causing national traffic paralysis, the closure of the metro system, the disruption of hospital operations, the disruption of all communication lines, the failure of flights to take off normal land and landing. To make it worse, there is an outage again on March 9th and 10th. According to statistics, the blackout is the longest power outage in Venezuela since 2012 as well as the world's longest-lasting national mass blackout incident [Tel19].

According to Venezuela's authorities, this is a man-made destruction incident. They believed the power plant was attacked by the US including a cyber-attack. There is no official statement about the event by now, but we can analyze the possible reason according to the public reports. Following are the three main causes of Venezuela blackout:

1. Lack of effective physical protection of key assets. According to the authorities, the Guri dam hydroelectric plant was attacked by combustion and explosion. We could speculate that the physical protection system may be disabled to protect infrastructure especially the information infrastructure.
2. Cyber-attack may be major cause. The supply and construction of key information infrastructure for the power plants is over-reliant on North American ICT providers and they may not implement effective preventive measures such as segmentation and IDS to the ICS. With many vulnerabilities and threats, the attacker can take advantage of the plant's monitoring system, seize the control right, operate the generator and get approach to cause the blackout.
3. Inadequate emergency response may also contribute to the huge loss. In view of the authorities' response when the incident occurred, we can speculate that emergency drill is also inadequate in the daily management leading to the poor management of emergency response in site.

6 Best Practices

Here, in this section, we provide recommendation for best practices for IIoT systems.

6.1 Review the Risk of Merging IT and OT

To operate properly, IIoT requires both IT and OT. However, both of them have totally different aims and considerations. While IT usually considers infrastructure, security, and governance, OT focuses on yield, quality, and efficiency [Fo17]. Furthermore, IT and OT have different methodologies regarding security, analyzing different risks, concentrating on different patching cycles, protocols, and etc.

6.2 Network Segmentation

Another possible risk is that attackers could gain access to industrial settings using other devices on the network. The attacker can use e.g., a phishing email to trick employees or insert malware to get an access into a network that is shared by office PCs and IIoT systems. IIoT systems must be appropriately segregated in the network. Therefore, devices and sensors that manage the pumps, valves, or any other device that is part of SCADA systems should be always connected on a completely separate network to the remaining IT infrastructure.

6.3 Evaluate Latest Cyber Threat Developments

As most IIoT devices contain default or no credentials, once malware gains access, it is spread quickly and affects other connected devices [Fo17]. Another rising threat is ransomware that recently started to attack IIoT devices. Furthermore, attackers are taking advantage and use old vulnerabilities on outdated devices that have not received security patches. Therefore, companies must keep up with most recent threat developments.

6.4 Secure Interoperability

The primary interoperability protocol for the implementation of Service Oriented Architecture (SOA) of Industry 4.0 is OPC Unified Architecture (OPC UA), as described in German Standardization Roadmap of Inustry 4.0 [Ge18]. This platform independent, scalable protocol is standardized by the multipart standard IEC 62541. IEC 62541-2 [IEC02] describes the security model for OPC UA. For IIoT systems that deploy this protocol, it is also important to enable and enforce the provided security measures. This is a challenge, as the protocol can be used for the Machine to Machine communication between factories and plant of different organizations with the IIoT devices located in different countries.

6.5 Appropriate Access Controls Schemes and Granularity

Often the granularity of current OT systems is very coarse. In some cases this may be due to convenience, e.g. by enabling security at the transport layer with OPC UA, but allowing all clients unlimited access to a given server. Typically current systems provide role based access control (RBAC) schemes combined with possibility to select groups of data (e.g. set-points) that can be accessed read-only or read-write. With critical infrastructure, that has to be accessed via the internet, a higher protection may be achieved with a finer access control granularity combined with conditions for the access, as supported e.g. by Attribute Based Access Control (ABAC) mechanisms.

6.6 Consideration of Legal Aspects in the Involved Countries

The M2M communication involve IIoT equipment located in facilites of different companies in different countries. Additionally, data may be centrally processed and backed up in cloud

environments hosted by computing centers operated by a third-party company. While this legal aspect does not concern the availability and integrity of information, it relates to the confidentiality, including the confidentiality of intellectual property and the key business values. For example, if not appropriately protected, a remote IIoT device may access data from a device located in another country. If for example the recipes and manufacturing procedures in a remote chemical plant are exposed (not protected at a different level), this may result in leaking of Intellectual Property. It may also result in the unnecessary storage of "important data" outside the national boundaries, which may incur penalties, depending the respective newest/applicable legislation. These challenges arne new, as the respective interoperability and Service Oriented Architectures were not yet in place before Industry 4.0.

6.7 Preparation of Secure Maintenance and Preventive Maintenance Procedures

Preventive maintenance can help asset owners and manufacturers to avoid losses (due to degrading assets) and business interrupts (e.g. due to timely ordering of replacement parts). With internet connectivity to factories and plants, considerable parts of the preventive maintenance and maintenance can be initiated from the Original Equipment Manufacturer (OEM) site or the Systems Integrator offices. This facilitates preventive maintenance by different OEMs and Integrators, to an extent that was not yet available before the deployment of IIoT equipment. The security aspects have to be considered when enabling the preventive maintenance and recurrent maintenance (e.g. by "over the air") application software and firmware updates.

6.8 Train Employees

All employees should receive cybersecurity training regularly. Any employee who would use IIoT solutions should be trained on at least basic security awareness topics before they obtain access to the system.

6.9 Emergency Response

Enterprises need to establish an emergency response agency, formulate an emergency response plan, and establish human resource measures such as an expert resource pool and a supporting manufacturer's resource pool. Equally, emergency drill is necessary to be carried out regularly, so that relevant partners know what to do in the event of an emergency.

7 Conclusion

Currently different cybersecurity standards are applied in the respective business domain. The fast market penetration of IIoT will make its way to the different domains. Cybersecurity has to consider the new challenges. As indicated in the recommendations, this seems to be best achievable by considering the industry domain specific cybersecurity standards

together with the cybersecurity standards that come with the new technology, e.g. to consider and enforce the security model of IEC 62541-2 [IEC02], when OPC UA is deployed. Additionally the new technical challenges, the legal aspects, the human (training) and the processes (e.g. preventive maintenance) have to be addressed.

The fast market penetration of IIoT has made and will continue to make its way to the different domains. The development of IIOT especially the merging of IT and OT would impose more new threats on enterprise information security and ICS security which will directly influence the production process. As indicated in the recommendations of best practices, we are dedicated to address the challenges from comprehensive consideration of the industry domain specific cybersecurity standards together with the cybersecurity standards that come with the new technology. Yet, specific measures need to be formulated and validated based on this guidance, which should also be improved constantly.

References

[Al] Alignment Report for Reference Architectural Model for Industrie 4.0 / Intelligent Manufacturing System Architecture. https://sci40.com/files/assets_sci40.com/img/sci40/Security%20Standards%20White%20Paper%20for%20Sino-German-Industrie%204.0.pdf.

[BQB17] Bochtler, Juergen; Quinn, Edward L.; Bajramovic, Edita: Development of a new IEC Standard on Cybersecurity Controls for Nuclear Power Plants. NPIC & HMIT, 2017.

[CL17] Cherepanov, Anton; Lipovsky, Robert: Industroyer: Biggest threat to industrial control systems since Stuxnet. 2017.

[Fo17] 9 best practices to improve security in industrial IoT. https://www.techrepublic.com/article/9-best-practices-to-improve-security-in-industrial-iot/.

[Ge18] German standardization roadmap. https://www.din.de/blob/65354/57218767bd6da1927b181b9f2a0d5b39/roadmap-i4-0-e-data.pdf#page=65, 2018.

[Go18] Good Practices for Security of Internet of Things in the context of Smart Manufacturing. ENISA, 2018.

[HR15] Hankel, Martin; Rexroth, Bosch: The reference architectural model industrie 4.0 (rami 4.0). ZVEI, 2:2, 2015.

[IE02] IEC 62264:2002, Enterprise-control System Integration, Part 1. Models and Terminology, Part 2: Model Object Attributes. International Electrotechnical Commission, 2002.

[IE09] IEC 62443-3-1:2009, Industrial communication networks Network and system security - Part 3-1: Security technologies for industrial automation and control systems. International Electrotechnical Commission, 2009.

[IE10] IEC 62443-2-1:2010, Industrial Communication Networks Network and System Security - Part 2-1: Establishing an Industrial Automation and Control System Security Program. International Electrotechnical Commission, 2010.

[IE15] IEC 62443-2-1:2015, Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment. International Electrotechnical Commission, 2015.

[IE18a] IEC 62443-2-2:2018 (Draft), Security for industrial automation and control systems - Part 2-2: IACS protection levels. International Electrotechnical Commission, 2018.

[IE18b] IEC 62443-4-1:2018, Security for industrial automation and control systems-Part 4–1: Secure product development lifecycle requirements. International Electrotechnical Commission, 2018.

[IEC02] IEC 62541-2:2016, OPC unified architecture - Part 2: Security Model. International Electrotechnical Commission, 2016.

[IEC09] IEC 62443-1-1:2009, Industrial communication networks—network and system security — part 1-1: terminology, concepts and models. International Electrotechnical Commission, 2009.

[IEC13] IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. International Electrotechnical Commission, 2013.

[IEC15] IEC 62443-4-2:2015, Security for IACS - Part 4-2: Technical security requirements for IACS components. International Electrotechnical Commission, 2015.

[IEE13] IEEE 1686:2013, Standard for Intelligent Electronic Devices Cyber Security Capabilities. IEEE, 2013.

[NER19] NERC CIP Standards. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[NI13] NIST, SP: , 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organization, 2013.

[NTT17] NTT Security 2017 Global Threat Report (GTIR). https://www.nttsecurity.com/en-us/gtir-2017.

[OK15] O'Halloran, Derek; Kvochko, Elena: Industrial internet of things: unleashing the potential of connected products and services. In: World Economic Forum. p. 40, 2015.

[Sc16] Schrecker, S; Soroush, H; Molina, J; LeBlanc, J: Industrial internet of things volume G4: security framework. Ind. Internet Consort, pp. 1–173, 2016.

[SP18] Schwab, Wolfgang; Poujol, Mathieu: The State of Industrial Cybersecurity Report 2018. Technical report, 2018.

[St15] Stouffer, Keith; Pillitteri, Victoria; Lightman, Suzanne; Abrams, Marshall; Hahn, Adam: Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, 2015.

[Tel19] Venezuela denounces US participation in electric sabotage. https://www.telesurenglish.net/news/Venezuela-Denounces-US-Participation-in-Electric-Sabotage-20190308-0021.html.

[Vo16] Voas, Jeffrey: Networks of 'Things'(NIST Special Publication 800-183). National Institute of Standards and Technology, 30:30, 2016.