Threat Analysis of Industrial Internet of Things Devices

Simon Liebl*, Leah Lathrop*, Ulrich Raithel†, Matthias Söllner* and Andreas Aßmuth*

*Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany,
Email: {s.liebl | l.lathrop | m.soellner | a.assmuth}@oth-aw.de
†SIPOS Aktorik GmbH, Altdorf, Germany, Email: ulrich.raithel@sipos.de

***Abstract*—As part of the Internet of Things, industrial devices are now also connected to cloud services. However, the connection to the Internet increases the risks for Industrial Control Systems. Therefore, a threat analysis is essential for these devices. In this paper, we examine Industrial Internet of Things devices, identify and rank different sources of threats and describe common threats and vulnerabilities. Finally, we recommend a procedure to carry out a threat analysis on these devices.**

***Keywords*—Threat analysis; Industrial Internet of Things; low-power devices; Cloud.**

I. Introduction

Approximately 20 billion Internet of Things (IoT) devices are in use today [1], and this number could double in the next five years [2]. The steadily increasing number of devices also raises the interest of attackers. During the first half of 2019, the overall number of cyberattacks increased by more than 350% compared to the previous six months [3]. The majority of attacks either aim to infect IoT devices or to launch attacks using them, such as Distributed Denial of Service (DDoS) attacks.

The increasing number of attacks also affects Industrial Internet of Things (IIoT) devices. These are IoT devices specialized on industrial applications and used in Industrial Control Systems (ICSs) for holistic monitoring and analysis using cloud computing. A common approach is to integrate the IIoT functionality into existing low-power Operational Technology (OT) devices. This can be recognized by the number of OT devices connected to a network. While about 60% of OT equipment was connected to the network in 2016, the figure had risen to almost 78% by 2018 [4].

ICSs are a frequent target for attacks. Recently, Microsoft security researchers discovered that the hacker group APT33 focuses specifically on manufacturers, suppliers and maintainers of ICS components [5]. OT devices installed in an ICS can cause extensive damage, since they control physical processes. The impact can be severe, especially in critical infrastructures, where this can result in a breakdown of power or water supply, for example. The increasing number of OT devices connected to the network, however, increases the attack surface of ICSs. As a result, it becomes easier for hackers to attack, successfully exploit OT devices and cause damage to ICSs.

Furthermore, the takeover of IIoT devices can also have an impact on cloud computing. In addition to the previously mentioned DDoS attacks on cloud servers, false data can be injected [6]. For example, ICS operators can be selectively supplied with incorrect information, e.g., abnormally high temperature values, to cause erroneous reactions, such as an emergency stop.

As a consequence of the increasing threats, IIoT manufacturers must secure their devices to prevent such incidents. This requires awareness of the risks. It is important to understand who is interested in exploiting their device and what motivates attackers to do so. In this paper, we aim to identify the threats specific to IIoT devices, describe how attackers could proceed and support IIoT manufacturers in conducting a threat analysis for their devices. The paper is structured as follows: in Section II, the differences between IoT, IIoT and OT devices are clarified and the use of IIoT devices in ICSs are described. Different types of threat sources and their respective intentions are introduced in Section IV. In Section V, several threats and vulnerabilities for IIoT devices are presented. A list of steps for a successful threat analysis follows in Section VI. The paper concludes in Section VII with an outlook on further work.

II. The Industrial Internet of Things

After a term differentiation, three potential setup options for a connection from IIoT devices to the cloud are described.

A. IoT, IIoT, OT and ICS

The IoT is a network of connected devices, which are sensors and/or actuators fulfilling a specific application [7]. Via the network they can, for instance, mutually exchange data or store and process data centrally and feed back the gained knowledge. This can be supported by cloud services. These have the advantage that there are already many semifinished solutions that simplify the integration of different devices. The number of devices or the required storage capacity can also be easily adapted, i.e., scalability. The use cases can be grouped in several categories, such as consumer applications (e.g., Smart Home), commercial (e.g., Medical and Healthcare) or infrastructure applications (e.g., Smart Grid). This paper focuses on industrial applications for which the already introduced term IIoT has been established. The main difference between IIoT and most IoT applications, such as consumer IoT, is that IoT services are human-centered and IIoT services are machine-oriented [8].

The use of IIoT devices can have various advantages, such as boosting productivity, avoiding plant downtimes through

 ISBN: 978-1-61208-778-8

predictive maintenance and reducing energy consumption. Furthermore, the IIoT should also enable products to be manufactured only after the order has been placed, i.e., build to order, and to be tracked by the customer during production and delivery. IIoT devices are usually part of the OT. OT can be found, for example, in industrial factories to monitor and control physical processes. The term was introduced to emphasize the significant difference to IT, such as field of application and used communication protocols. Some examples for OT/IIoT sensors are temperature probes or bar code scanners, actuators are, for instance, valves or power converter. The primary security challenges for IoT devices are privacy and confidentiality, e.g., human health data. However, IIoT devices focus additionally on safety and the impact on environment and society [9]. They can potentially cause injury, death, damaged production equipment or environmental disasters. This can also affect large parts of the population through critical infrastructures, such as food or health.

An ICS is usually structured into several layers. The lower levels are made up of OT devices and Programmable Logic Controllers (PLCs). The middle layers contain, for example, Human Machine Interfaces (HMIs) and engineering workstations. The top levels provide servers for services and backups. An increase in security can be achieved by dividing the ICS into multiple layers so that more protection can be provided to the lowest level, which is especially safety-critical. This concept is known as defense in depth. Another approach is air gapping, isolating the entire ICS network from the Internet or even corporate network. It has been demonstrated that particularly the latter does not provide sufficient security. Nevertheless, both measures result in more complex and expensive attacks. First, the IT network must be compromised (e.g., via email intrusion), then malware must be transferred to the OT network (e.g., via USB sticks) and, lastly, malicious code must be transferred to the PLCs [10]. Once this is achieved, systems be controlled, damaged or spied on. However, these approaches conflict with the IIoT functionality of OT devices, as the lowest level requires Internet access. As a result, the architecture of ICS networks is affected by IIoT devices.

B. Cloud Connection Setups

Several IoT/IIoT architectures have already been proposed to implement segmented and logically structured networks [11]. In reality, however, these architectures can differ significantly. Therefore, different setups are only considered in an abstract way. The characteristics of a device, the task it performs and the level it is located on are important for the threat analysis.

Figure 1 illustrates three possible setups. In small ones, each device can be connected separately to clouds. This could be, for example, a small, remote hydroelectric power plant connected to the Internet via mobile networks. The proprietary firmware of valves has been extended by a network stack for this purpose. The devices are connected to the operator's cloud for centralized monitoring and controlling and to the device manufacturer's cloud service for installing remote firmware updates.

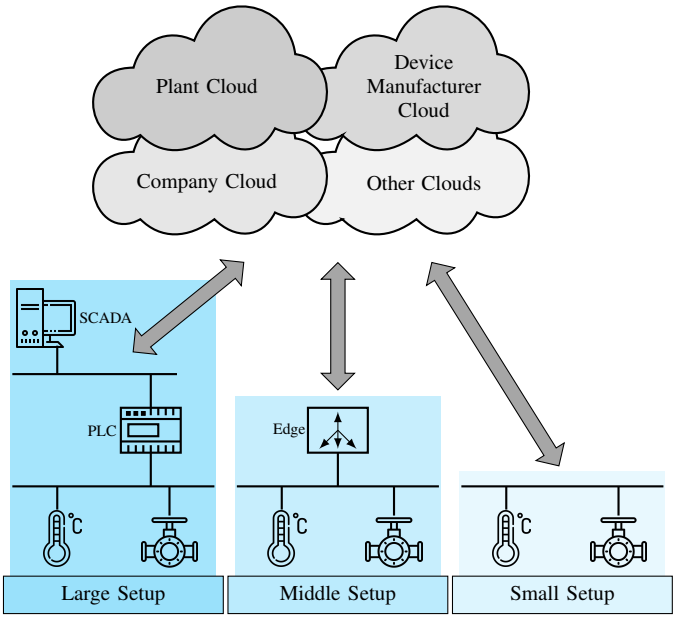

Figure 1. Three possible setups for connections from IIoT devices to clouds.

In the middle setup, devices are connected to the cloud via an edge gateway. It is not unusual for industrial devices to be older than ten years. They were not designed to send data to the cloud. Therefore, gateways collect data from several devices over mostly proprietary protocols, such as CAN or Modbus. Compared to low-power field devices, gateways have a more powerful processor and often a Linux-based operating system.

Even entire Supervisory Control And Data Acquisition (SCADA) systems are outsourced to the cloud in large industrial factories. Flexible web interfaces for desktops and mobile devices allow remote monitoring and control of the entire plant. In this scenario, many more connections to the cloud are possible, e.g., when the numerous field devices connect to their manufacturer's cloud or when all plants are combined in a company cloud.

III. Related Work

Since many IoT device manufacturers often prioritize functionality and time to market, security is neglected or not considered. This has been recognized by researchers and governmental institutions, leading to active research on the threats, necessary security requirements and mitigation techniques.

The German Federal Office for Information Security (BSI) releases annually an Information Security Management System (ISMS), the so-called IT-Grundschutz Compendium, that covers, among others, technical and organizational aspects of information security [12]. The aspects are divided into several modules. For example, embedded devices (SYS.4.3), IoT devices (SYS.4.4) and ICS components (IND.2.1) are modules concerning threats and the resulting requirements.

 ISBN: 978-1-61208-778-8

In [13], Abomhara et al. evaluate IoT device attacks, vulnerabilities, assets and possible intruders. Although industrial systems, such as SCADA systems, are mentioned, the special characteristics of ICSs are not described in depth. In [14], Wurm et al. conducted a security analysis on a consumer IoT and an IIoT device and demonstrated how these devices could be exploited. However, the procedure is too specific and cannot be adapted to other devices.

So far, manufacturers are assisted by standards and scientific papers in conducting a threat analysis for any system. However, there are no mandatory international guidelines on how the analysis should be carried out. In addition, computer-based threat modeling tools are not suitable for the special conditions of IIoT devices.

IV. Threat Sources and Motives

To protect IoT devices from unauthorized access, it is helpful to know who is interested in using them, i.e., the threat sources. Depending on application and device characteristics, the sources can be different. For instance, IIoT applications in critical infrastructures are more likely to be attacked by Advanced Persistent Threat (APT) groups, whereas IoT devices with open Telnet or SSH ports are favored by botnet operators. Generally, there are also threats caused by natural disasters or unintentional misuse by employees, but these will not be considered in this paper. We have classified the sources based on two characteristics. First, to what extent the attack targets were selected arbitrarily or intentionally. Second, what capabilities attackers have, i.e., how many skills and financial resources are available to them. Figure 2 classifies nine threat sources accordingly. In the following section, each source is described in detail.

A. Targeted attacks and capable attackers

a) Government-Sponsored: The most serious threat arises when an ICS is the target of attackers who are supported by a government or agency. Examples include the attacks on the Iranian nuclear program (Stuxnet) [15] or on the Ukrainian power grid [16], both of which are suspected to have been supported by foreign governments. The attacks were targeted and only possible at high expense due to their complexity. The motives to conduct such attacks are usually political or economical.

b) Industrial Espionage: Economic reasons are generally a major motive. Targeted attacks aim, for example, to sniff production figures, customer data and know-how, or simply cause financial loss to competitors. In recent years, there were several espionage attacks on German companies of the DAX (German stock index), including the ICS component manufacturer Siemens [17].

B. Less targeted attacks, but capable attackers

a) Organized Crime: Organized cybercriminals try to blackmail their victims by encrypting sensitive data. The recently discovered ransomware EKANS seems to be specifically intended for ICSs because it terminates several common ICS-specific software processes [18].

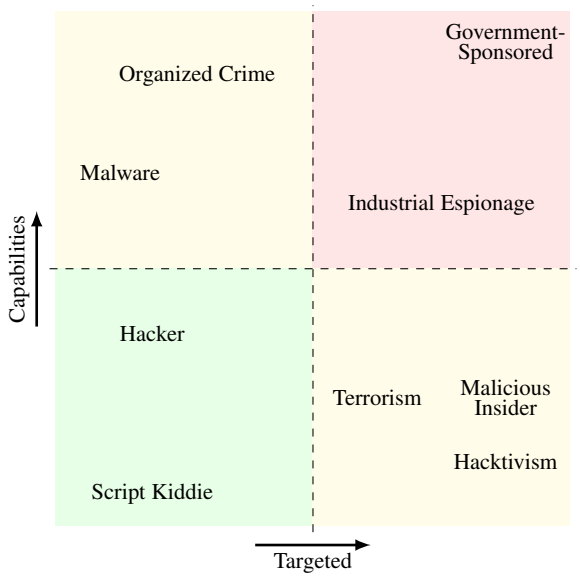

Figure 2. Threat Sources.

b) Malware: Malware is often designed to infect as many devices as possible, for instance, to build botnets. Mirai and its many variants demonstrated that millions of IoT devices are vulnerable to malware attacks [19].

C. Targeted attacks, but less capable attackers

a) Terrorism: Threats from terrorism can be considered from two perspectives. There is a threat from extremist organizations. Although they are theoretically capable of carrying out attacks, few attacks are known in practice [20]. Additionally, terrorism can also be sponsored by states. Attacks on critical infrastructures, such as energy or water, affect the general civilian population. Therefore, they are a kind of terrorism. Since government-sponsored threats are already covered, the capabilities of terrorism is rated low.

b) Malicious Insider: Insider attacks by (former) employees or contractors cause an average annual loss of more than eight million dollars [21]. Employees, for example, could sell confidential data for personal financial gain or sabotage machines due to hostility towards the employer. They also possess specialist knowledge, which is particularly required for attacks on IIoT devices. Insider attacks are the major threat to OT [22], especially for ICSs in critical infrastructures, as identified by an evaluation of US hydropower dams [23].

c) Hacktivism: The number of attacks by hacktivists is increasing and should therefore not be neglected. The attacks are targeted, but have not frequently been effective so far. Besides DoS attacks, attempts are made to steal data. This could affect, for instance, oil and gas companies or companies that make politically controversial decisions. The latter happened to heavy machinery maker Caterpillar Inc. as a result of the sale of bulldozers to Israel [24].

 ISBN: 978-1-61208-778-8

D. Less targeted attacks and less capable attackers

a) Hacker and Script Kiddie: The last two threat sources we identified are hackers and script kiddies. The source code of malware, e.g., Mirai, is frequently published on code sharing platforms like Github or hacker forums. As a result, many people want to try them out for themselves. Compared to script kiddies, experienced hackers can build on this code and develop their own variants.

V. Threats, Vulnerabilities and their Impact

Several threats were already mentioned in the listing of threat sources. In the following section, the threats are summarized briefly and common vulnerabilities are described. Possible attack vectors on IIoT devices are illustrated afterwards. Table I provides an overview of frequent threats and vulnerabilities for IIoT devices.

TABLE I. Common threats and vulnerabilities.

Threats	Vulnerabilities
Abuse	Code execution
Denial of Service	Communication manipulation
Destruction	Design flaws and bugs
Espionage	Memory manipulation
Intellectual property theft	Misconfiguration
Maloperation	Physical manipulation
Ransomware	Privilege escalation
Repudiation	Repudiation
Spoofing	Web-based vulnerabilities

A. Threats

a) Abuse: The source of this threat could be malware or employees. The former utilizes IIoT devices as part of a botnet for DoS attacks, mining cryptocurrencies or for spreading spam. The latter could use the device for private purposes.

b) Denial of Service: For ICS operators, the availability of all devices is most important because a single temporary breakdown can potentially lead to a production stop. Therefore, the failure of a device could have financial consequences for operators. A denial of service can be achieved not only by flooding devices with network requests but also by changing their configuration. Multiple devices could also be utilized to stop cloud servers. This would not only block one plant from its cloud services but all other plants of a large company.

c) Destruction: The destruction of a device is also a form of denial of service, more precisely a permanent denial of service. The attack can be either on hardware or software. An example of the latter is BrickerBot, which destroyed more than ten million IoT devices [25]. Furthermore, the actuators of an OT device can be incorrectly triggered, destroying components, such as engines. The consequences are far more serious than a normal DoS attack. If there is no backup device that takes over immediately, the plant is out of operation. Additionally, data saved on the device may be lost.

d) Espionage: Espionage was already introduced in Section IV. Stealing production data, process procedures or even user data is often easy because many industrial communication protocols are not encrypted at all.

e) Intellectual property theft: OT devices are usually specialized on one specific task. Manufacturers invest a lot of effort into their product in order to be better than competitors. As a result, leading manufacturers struggle with plagiarism and cloned, cheaply replicated hardware that runs their original firmware.

f) Maloperation: Starting or stopping machines unexpectedly or making them work in slightly different ways is not a theoretical issue anymore. Two recent examples are TRITON [26] and Industroyer [27] that were specifically created for OT devices and protocols. The latter supports four industrial communication protocols and is capable of controlling switches and circuit breakers in electricity substations.

g) Ransomware: If, in addition to the IT network, the OT network is also affected by a ransomware attack, some machines in the plant may no longer be available. As a result, the ICS must be shut down. This incident happened recently to a pipeline operator, who had to shut its operation down for two days, according to a report by the US Cybersecurity and Infrastructure Security Agency (CISA) [28].

h) Repudiation: In case of an error in an ICS, it should be possible to reconstruct the exact procedure with logs. Attackers could manipulate or delete them in order to remain undetected.

i) Spoofing: IIoT devices must be uniquely identifiable. Attackers could masquerade as the device and send false data to PLCs or cloud services. The latest firmware could also be obtained by cloning original devices and spoofing their identity.

B. Vulnerabilities

a) Code execution: Arbitrary code execution is the goal of every attacker. Attacks can be either local or remote. Since the firmware of IIoT devices is mostly written in C/C++, they are vulnerable to memory attacks, such as buffer overflows.

b) Communication manipulation: Message senders or receivers, measured values or commands can be easily manipulated due to unencrypted communication.

c) Design flaws and bugs: Many industrial devices and protocols were not designed with security in mind. Even if this is the case, bugs can still occur. An example of this is the encrypted OPC UA protocol, which contained numerous flaws [29]. This is particularly critical in ICSs because the firmware of the countless devices is rarely or never updated.

d) Memory manipulation: By manipulating the memory, incorrect configurations can be loaded, faulty data can lead to inappropriate reactions and features that would be subject to additional costs can be unlocked illicitly.

e) Misconfiguration: Misconfigurations enable many attacks. Common mistakes are unchanged default passwords, disabled firmware patches and open but unused ports.

f) Physical manipulation: Attackers with physical access to IIoT devices can alter the hardware, e.g., sensors or actuators but also microcontrollers or memories.

g) Privilege escalation: Some actions should only be executed with higher privileges. For IIoT devices it is often

 ISBN: 978-1-61208-778-8

simple to obtain these due to standard or company-wide passwords or backdoors of the developers. Furthermore, most industrial protocols do not support authentication. Therefore, it is not possible to verify authorization for them.

h) Repudiation: The aforementioned threat is also a vulnerability, since insufficient logging and monitoring hinders the detection and verification of threats. Due to lack of identification mechanisms, actions can be easily repudiated.

i) Web-based vulnerabilities: IIoT devices often run a web server for configuration, maintenance, monitoring or control of the devices. But this exposes them to web-based attacks. According to OWASP, the greatest risks include injection, broken authentication and cross-site scripting (XSS) among others [30].

C. Attack Vectors

IIoT devices are becoming increasingly complex. As a result of the IoT, new communication interfaces are being integrated that were previously rarely or never used in OT. In any case, they provide typically several interfaces for specific requirements. For better illustration, we have structured the various interfaces into zones in Figure 3. Zones 0 and 1 describe the hardware and software of a device. In zones 2 to 4, established communication protocols are listed in the left-hand column while systems that interact with them are listed in the right-hand column.

In the following section, three possible attack vectors are introduced. Examples are used to illustrate how attackers from the different zones could proceed or how they could have an impact on other devices in these zones.

a) Device attacks: In zone 0, device components can be physically manipulated. This may be intentional or accidental. In the latter case, a burnt-out circuit board or a defective engine could be replaced by a spare part that was not purchased from the original manufacturer for price reasons. Compatibility of hardware or software is not guaranteed for these components causing faulty operation, DoS and even destruction to result.

As discussed in Section IV, IIoT devices are especially threatened by highly capable actors. Attacks with high complexity and effort should consequently not be ignored. Costly invasive hardware attacks, such as probing, or rather cheaper non-invasive attacks, such as side-channel analysis, enable access to secret data, e.g., cryptographic keys. Attackers can also directly access the flash memory or EEPROM via interfaces from zone 2, e.g., JTAG. First, this allows them to read the memory to retrieve the firmware, i.e., intellectual property theft. Second, data or configurations can be modified, e.g., access data. Third, firmware can be exchanged so that arbitrary code can be executed. Attacks of this kind are complex, but they can cause considerable damage. In case the necessary knowledge is lacking, there are appropriate service providers for this (e.g., www.break-ic.com).

The popular USB interface also enables multiple attacks. USB sticks can be used, for example, to load malware or destroy badly protected power and data lines, i.e., kill USB sticks. With bad usb devices, such as Hak5's rubber duckies,

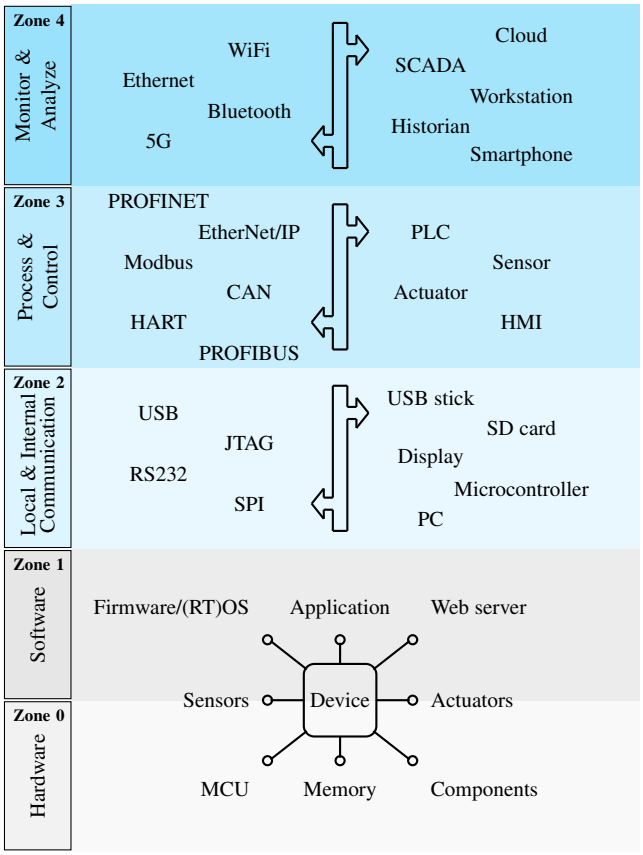

Figure 3. Different zones of a device and their respective interfaces with interaction systems.

it is also possible to execute arbitrary commands and thus manipulate the device.

b) Application attacks: The process of a production plant can be interrupted or stopped if the application of IIoT devices do not work properly. An attacker might change the configuration or move an actuator incorrectly via its display. The devices are often misconfigured as they still have the default or a trivial password. Many IIoT devices can also be programmed using a PC-based configuration tool. A common design flaw is that users must not be authorized to carry out these changes. As a result, it is often possible to reconfigure, update or reset a device by connecting to it via a cable or network. When such a vulnerability is exploited, it is difficult to reconstruct and verify the incident, as the devices often do not support user identification.

Wrong commands can also originate from the devices of zone 3. The source can be either an already compromised PLC or a completely different device. Since messages of the most proprietary protocols are not authenticated, a different sender address can be spoofed. Reversely, incorrect information can also be sent to PLCs or HMIs. For example, PLCs from the manufacturer Schneider can be stopped using a simple command via the Modbus protocol [31]. The consequences of this abrupt stop may be catastrophic. Faulty commands or sensor data can also be sent to systems in zone 4, e.g., the SCADA system or the cloud. Since more decisions will be

 ISBN: 978-1-61208-778-8

made by a data-driven Artificial Intelligence (AI) in the future, wrong choices may result.

Due to the more widespread network protocols in zone 4, vulnerabilities can also be exploited remotely. Such vulnerabilities can be located in the firmware/operating system or the application. An example of the former are the Treck TCP/IP stack vulnerabilities called Ripple20 that allow remote code execution, which were recently discovered [32]. Vulnerabilities in the application can be caused by a web server that allows SQL injection, for instance. Once they have successfully exploited a vulnerability, process operations can be sabotaged.

c) Network attacks: The vulnerabilities just mentioned also allow an infection of botnets. If several devices in a network are infected and the botnet operator launches a DDoS attack, internal network traffic can be delayed. This can, for example, interrupt the connection of PLCs to the SCADA system. In case the attack is targeted at the own global company cloud, other plants might be affected as well.

If the device is a network node, such as an edge device, this also results in multiple threats. Besides sniffing or tampering with messages, they can also be delayed or blocked. Especially for systems that have to meet real-time constraints, this can become a major threat.

The network is also useful for spreading an infection. Especially the systems in zone 4 are targeted either for monetary gain through a ransomware attack or to obtain as much control as possible. Workstations with Win 7 or Win XP are not rare in ICSs, and thus this is often not much effort for an attacker.

VI. Recommended Procedure

Finally, we summarize all the previously discussed aspects to define a recommended procedure for the threat analysis.

1) Know your device: It is important to know the IIoT device in depth. Which operating system and third party libraries are utilized? Does it include actuators and sensors and/or is it collecting data from other devices (i.e., edge device)? How is the setup? What other equipment is connected to it? Is it connected to the Internet directly or through a gateway? Is it installed in critical infrastructures? What additional (PC-)tools are available for the device?

2) Creation of a network diagram: A network diagram including all interfaces of the device can help identify which other systems it interacts with. The authorization should be specified for each entry and exit point, i.e., which actions can be performed and by whom. This is especially important for industrial protocols, such as PROFINET. While most IoT applications allow to implement security measures manually, it is not possible with these proprietary protocols.

3) Identification and ranking of assets: Which security goal is the most important one? Is the focus on maximum availability, authenticity of actions or privacy of user data? First, this is important to prioritize the exploration of vulnerabilities, and second, to subsequently find an appropriate mitigation measure. The latter is particularly relevant when safety must be guaranteed, as real-time behavior and encryption may not be feasible on a low-power IIoT device.

4) Identification of threat sources: Who is interested in attacking the device and what are their motives? This is useful for deliberately including or excluding types of attacks. For IIoT devices in critical infrastructures, the more complex invasive and non-invasive hardware attacks should be addressed.

5) Identification of threats and vulnerabilities: The next step is to identify threats and vulnerabilities. Table I serves as a kick-off aid. In general, we can consider attacks on identification and authentication, authorization, availability, system, data and communication integrity, data confidentiality, privilege escalation and repudiation. Penetration testing can be used to discover additional vulnerabilities, but also to verify those already identified and show their severity.

Using attack scenarios, attacks can be better reconstructed in retrospect. For example, the threat *setting an invalid communication configuration* results in a *denial of service*. The attack vector is that the *web server* is accessible via the *Ethernet* interface. The action *changing of communication parameter* has the consequence that the *connection to PLCs is terminated*. The utilized vulnerability is a *default password* that results in a *privilege escalation*. Additional notes, such as *default password can be found in the manual*, can also be useful.

6) Vulnerability and risk assessment: To rate a vulnerability, all threats and their consequences from the different attack scenarios should be considered. Using the Common Vulnerability Scoring System (CVSS), the severity of vulnerabilities can be expressed by a number. For risk assessment, it is advisable to consider not only the severity of the vulnerability but also its likelihood and impact.

VII. Conclusion and Further Work

Compared to IoT equipment, IIoT devices are at increased risk, since they are part of the OT that controls physical processes. Beside high availability, safety is also particularly important in these applications. In addition to destroying a production facility, people can be injured and a population can even be cut off from the power grid.

Several threat sources and their motives were presented and ranked using examples. It turned out that the most serious threat originates from government-sponsored actors, who often target critical infrastructures. Afterwards, numerous threats and vulnerabilities were listed, which exist among other reasons, because security was ignored in the industrial sector for decades. Among the threats, destruction caused by moving parts and intellectual property theft must be highlighted, while the vulnerabilities include manipulation of the hardware and the frequently insecure communication. Lastly, we provided a procedure for identifying and assessing threats and vulnerabilities that emphasizes the specialties of IIoT devices. In order to prevent these, we intend to develop countermeasures for low-power IIoT devices as the next step.

Acknowledgment

The research project “Intelligent Security for Electrical Actuators and Converters in Critical Infrastructures (iSEC)”

is a collaboration of SIPOS Aktorik GmbH, Grass Power Electronics GmbH and OTH Amberg-Weiden. It is supported and funded by the Bavarian Ministry of Economic Affairs, Regional Development and Energy.

REFERENCES

[1] M. Hung, "Leading the IoT: Gartner Insights on How to Lead in a Connected World," Gartner, White Paper, 2017.

[2] IDC Corporate USA, "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast," June 18th, 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219 [accessed: 2020-08-25]

[3] F-Secure, "Attack Landscape H1 2019," 2019. [Online]. Available: https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf [accessed: 2020-08-25]

[4] J. Santagate, R. Glaisner, and R. Westervelt, "Operational Cybersecurity for Digitized Manufacturing: Emerging Approaches for the Converged Physical-Virtual Environment," IDC, 2019. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-idc-operational-cybersecurity-for-digitized-manufacturing.pdf [accessed: 2020-08-25]

[5] A. Greenberg, "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems," Wired, November 20th, 2019. [Online]. Available: https://wired.com/story/iran-apt33-industrial-control-systems/ [accessed: 2020-08-25]

[6] B. Bostami, M. Ahmed, and S. Choudhury, "False Data Injection Attacks in Internet of Things," in Performability in Internet of Things, F. Al-Turjman, Ed. Cham: Springer International Publishing, 2019, pp. 47–58.

[7] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "Internet of Things: A Definition & Taxonomy," in 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, United Kingdom, 2015, pp. 72–77.

[8] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," IEEE Trans. Ind. Inf., vol. 14, no. 11, pp. 4724–4734, Nov. 2018, DOI: 10.1109/TII.2018.2852491.

[9] A. Hahn, "Operational Technology and Information Technology in Industrial Control Systems," in Cyber-security of SCADA and Other Industrial Control Systems, 2016, pp. 51–68, DOI: 10.1007/978-3-319-32125-7_4.

[10] Symantec, "Internet of Things: Protecting Against Industrial Cyber Attacks," 2018. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/brochures/internet-of-things-protecting-against-industrial-cyber-attacks-en.pdf [accessed: 2020-08-25]

[11] H. P. Breivold, "A Survey and Analysis of Reference Architectures for the Internet-of-things," in The Twelfth International Conference on Software Engineering Advances, 2017, pp. 132-138.

[12] Federal Office for Information Security, Ed., "IT-Grundschutz Compendium" (IT General Protection Compendium), 2019.

[13] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, 2015.

[14] J. Wurm, K. Hoang, O. Arias, A. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macau, 2016, pp. 519-524, DOI: 10.1109/ASPDAC.2016.7428064.

[15] E. Nakashima and J. Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," The Washington Post, June 2nd, 2012. [Online]. Available: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html [accessed: 2020-08-25]

[16] R. Lee, M. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC, 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [accessed: 2020-08-25]

[17] H. Tanriverdi, S. Eckert, J. Strozyk, M. Zierer, and R. Ciesielski, "Attacking the Heart of the German Industry," BR, July 24th, 2019. [Online]. Available: https://web.br.de/interaktiv/winnti/english/ [accessed: 2020-08-25]

[18] A. Greenberg, "Mysterious New Ransomware Targets Industrial Control Systems," Wired, February 3rd, 2020. [Online]. Available: https://wired.com/story/ekans-ransomware-industrial-control-systems/ [accessed: 2020-08-25]

[19] C. Cimpanu, "A decade of malware: Top botnets of the 2010s," Wired, December 3rd, 2019. [Online]. Available: https://www.zdnet.com/article/a-decade-of-malware-top-botnets-of-the-2010s/ [accessed: 2020-08-25]

[20] S. Sin, E. Asiamah, L. Blackerby, and R. Washburn, "Determining Extremist Organisations' Likelihood of Conducting Cyber Attacks," presented at the 8th International Conference on Cyber Conflict, Tallinn, 2016.

[21] Ponemon Institute, "2018 Cost of Insider Threats: Global," April, 2018. [Online]. Available: https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/ObserveIT-Insider-Threat-Global-Report-FINAL.pdf [accessed: 2020-08-25]

[22] Siemens, "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?," 2019. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf [accessed: 2020-08-25]

[23] U.S. Department of the Interior Office of Inspector General, "U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk from Insider Threats," June, 2018. [Online]. Available: https://www.hsdl.org/?view&did=829751 [accessed: 2020-08-25]

[24] K. Fazzini, "Rising Hacktivist Attacks Take Companies By Surprise," Dow Jones, April 4th, 2017. [Online]. Available: https://dowjones.com/insights/rising-hacktivist-attacks-take-companies-surprise/ [accessed: 2020-08-25]

[25] radware, "'BrickerBot' Results In PDoS Attack," 2018. [Online]. Available: https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/ [accessed: 2020-08-25]

[26] S. Miller, N. Brubaker, D. Kapellmann Zafra, and D. Caban, "TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping," FireEye, April 10th, 2019. [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html [accessed: 2020-08-25]

[27] A. Cherepanov and R. Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet," welivesecurity, June 12th, 2017. [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ [accessed: 2020-08-25]

[28] Cybersecurity and Infrastructure Security Agency (CISA), "Ransomware Impacting Pipeline Operations," February 18th, 2020. [Online]. Available: https://www.us-cert.gov/ncas/alerts/aa20-049a [accessed: 2020-08-25]

[29] Kaspersky, "Kaspersky Lab discovers critical vulnerabilities in popular industrial protocol, affecting products from multiple vendors," May 10th, 2018. [Online]. Available: https://www.kaspersky.com/about/press-releases/2018_kaspersky-lab-discovers-critical-vulnerabilities-in-popular-industrial-protocol [accessed: 2020-08-25]

[30] OWASP, "OWASP Top 10 - 2017," 2017. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_(en).pdf.pdf [accessed: 2020-08-25]

[31] C. E. Bodungen, B. L. Singer, A. Shbeeb, S. Hilt, and K. Wilhoit, Hacking exposed, industrial control systems: ICS and SCADA security secrets & solutions. New York Chicago San Francisco: Mc Graw Hill Education, 2017, p.146.

[32] M. Kol and S. Oberman, "Ripple20," JSOF, White Paper, 2020. [Online]. Available: https://www.jsof-tech.com/wp-content/uploads/2020/06/JSOF_Ripple20_Technical_Whitepaper_June20.pdf [accessed: 2020-08-25]

 ISBN: 978-1-61208-778-8