Fraunhofer

Cybersecurity lab to promote security in the manufacturing industry

Alexander Kreppein, Robert H. Schmitt
DOI: 10.24406/h-442705

Extract from:
ICNAP Study Report 2022
International Center for Networked, Adaptive Production, Aachen
DOI: 10.24406/publica-1262

Cybersecurity lab to promote security in the manufacturing industry

Alexander Kreppein
Research Fellow
Production Quality
Fraunhofer Institute for Production Technology IPT

Prof. Dr.-Ing. Robert H. Schmitt
Member of the board of directors of Fraunhofer IPT and holder of the chair for Production Metrology and Quality Management at the WZL of RWTH Aachen University

Introduction

Dealing securely with cyber related risks is a crucial factor in the successful design of a networked production in the manufacturing sector. In an online survey of 500 security experts in the U.S., Germany, and Japan, more than 60 percent stated that they had experienced cyberattacks and seventy percent of incidents resulted in system outages [43]. The number of such attacks is increasing. In 2021, the manufacturing sector replaced the finance sector as the most attacked in Europe [44]. The targets of these attacks are not only large companies, but also small and medium-sized enterprises, which are often inadequately protected [45]. In the event of a successful attack, the effects are often severe, with one in four companies with fewer than 50 employees even suffering consequences that threaten their existence [46].

The fact that the manufacturing sector in particular falls victim to cyber-attacks can be explained by the historical separation of Information Technology (IT) and Operation Technology (OT). While IT is responsible for handling business data and information, OT takes care of monitoring and controlling physical production processes. In networked production, the boundaries between IT and OT are becoming increasingly blurred, so OT must also become part of a security concept. OT is often considered to play a subordinate role and was neglected in the development of hardware and software components. Because established security concepts from IT can only be transferred to OT to a limited extent, security gaps in OT are common practice in the manufacturing sector. At the same time, networking and digitization projects are creating additional interfaces in OT, which, without a security concept, can become a gateway for attackers. Companies are skeptical about networking and digitization initiatives because of the increasing number of attacks and digitalization projects creating new attack surfaces is one of the reasons why. However, companies should not postpone digital transformation due to concerns about cyberattacks but should instead use the potential of digitized manufacturing while being protected with a robust security concept.

This study is concerned with the challenge presented to companies to select and implement suitable security concepts that provide an effective protection against cyber-attacks. For this purpose, a cybersecurity lab was built to demonstrate how attackers can infiltrate a production network and which damages they can cause. Based on these results, a security guideline was developed to provide help for the implementation of effective protection measures. The study provides theoretical knowledge about security concepts as well as best practices and use cases to address a broad audience of interested ICNAP community members by answering the research question "How can companies select and implement suitable cybersecurity technologies for their production?".

The following chapters are structed as follows: First, security measures are presented by introducing security concepts, security application areas, and the security framework introduced by the National Institute of Standards and Technology (NIST). Finally, a conclusion is given with a summary of the conducted study and a discussion of possible next steps.

Security Guideline

The security guideline consists of three steps (see Figure 16). Beginning with the first step of the guideline, the security strategy Defense-in-Depth is presented. The second step consists of application areas: processes, organization, people, and technology. Finally, the last step consists of the security framework of the National Institute of Standards and Technology (NIST), which developed a five-step process to incorporate security measures into operational technology.

Security strategy

Defense-in-Depth (DiD) is a security strategy that consists of a series of security mechanisms and controls for information and operational technologies. The main idea of DiD is the layered protection of valuable assets. Each layer adds one or more security mechanism to protect the asset. This multi-layered approach provides security redundancies that protect the asset even in a case of one security mechanism failing. The different layers include (see Figure 17):

1. Policies & Risk Management: Risk Management defines the most relevant assets and attack vectors to consider. Policies are used to implement security guidelines and practices in the organization and include reaction processes in case of an attack.
2. Human Component: Cyber-attacks often start by targeting humans. Protection measures for employees range from awareness training up to in-depth security trainings for OT security responsible employees.
3. Physical Security: Physical security can range from physical protection measures for the production plant to security solutions to prevent unauthorized access to restricted areas, such as server rooms.
4. Network Security: The network security includes the protection of IT & OT networks which are created to connect different systems and components. Detecting attacks is also an important task within network security.
5. System & Component Security: System & components include endpoints such as industrial computers, edge devices, or PLCs that are used to monitor or control the operations.
6. Asset: The assets differ from company to company. In general, an asset in OT security is physical equipment (e. g. a machine), data that contains valuable knowledge (e. g. Computer-aided Designs, CAD), or software (e. g. Manufacturing Executing System, MES).

Application areas

When considering OT security measures, technical solutions offer only one of four action areas. It is equally important to consider the organization itself, its processes, and the people within the organization (see Figure 18). In the area of technology, suitable measures depend on the criticality of the assets.

Security framework

The National Institute of Standards and Technology (NIST) created a framework for IT-security in 2013. Until today, the framework has received several updates and in April 2022, the first draft of a "Guide to Operational Technology (OT) Security" was introduced [47]. This chapter introduces the most relevant tasks for manufacturing companies based on the NIST Framework and the "Guide to OT Security" (see Figure 19). These frameworks were selected because of their specific focus on Operational Technology and their practical examples and recommendations. The framework consists of five phases that structure the following chapter.

Figure 16: Three steps of the ICNAP security guideline

Identify

The phase 'Identify' consists of several task, with the most important ones being Asset Management and Risk Management.

For organizations, asset management provides transparency about which assets need to be protected. A clear definition about what an asset is does not exist, so that organizations must propose an individual specification. In the context of operational technologies, an asset can generally consist of physical objects (e.g. a machine tool) or digital objects (e.g. a managed switch). Decisive factors for the classification are the usage, the requirement, and the circle of users of the assets. The special publication of the NIST "Guide to Operational Technology (OT) Security" suggest an asset management to consistently identify and update data, personal, server, and devices [47]. To support organizations with this task, the following tasks are recommended:

- Use of unique identifiers to track assets
- Track computing and networking devices including their locations and details such as vendor, model, serial number, and purchase information
- Track software and firmware inventory management [47]

Risk Management is usually performed as one of the first steps to identify security risks in an OT environment. Due to its importance for OT-security, NIST introduced the special publication 800-30 "Guide for Conducting Risk Assessment". This guide recommends a four-step process: Prepare for Assessment, Conduct Assessment, Communicate Results, Maintain Assessment. The goal of the first step is to establish a context for the risk assessment and identifying the purpose, scope, assumptions and constraints, source of information, and the risk model. The second step, "Conducting the Risk Assessment," is the main part of the four-step process which aims to produce a list of prioritized security risks. To accomplish this task an organization must analyze threats and vulnerabilities, impacts and likelihoods, and the uncertainty associated with the risk assessment. The last two steps of the process, "Communicate Results" and "Maintain Assessment", aim to share information about the prioritized security risks to decision makers in the organization and to support the ongoing review of the risk management process [48].

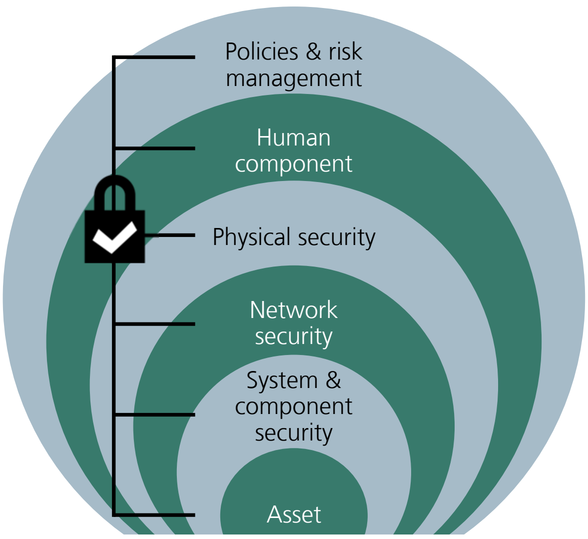

Figure 17: Defense-in-Depth strategy

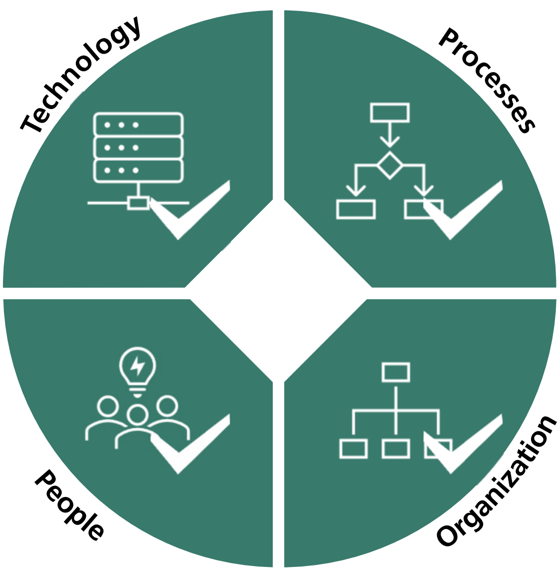

Figure 18: Application areas for OT-security

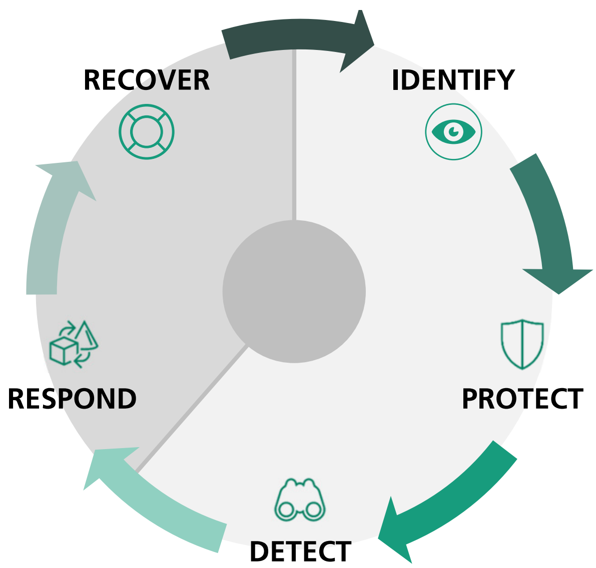

Figure 19: Five phases of the NIST security framework

Protect

After identifying threats to the operational technology, the goal of the second phase of the NIST Framework is to develop and implement the appropriate safeguards to ensure delivery of services [49].

Access Control: Managing who has access to which information and equipment is a crucial step towards OT-Security. This can limit the abuse of an external attacker on a user account and the internal abuse caused by an inside-attacker. Therefore, accounts should be individually created for every employee and grant access only to information, computers, and applications that are needed for their job. Authentication should ideally be based on a multi-factor technique.

Device Hardening: Devices used in an OT-Environment are often legacy devices with outdated operating systems, patches, and software. To improve security for those devices, updates to the newest versions are recommended. However, in OT applications this is often not as easy as in an IT environment, due to tight availability requirements or outdated hardware. Therefore, back-ups should be made regularly and especially before an update attempt. Installing updates should be performed during maintenance intervals. If an outdated hardware prevents the installation of security updates, the hardware should not be allowed to communicate in the OT-Network without additional measures. Solutions are described in the next protection measure 'device networking'.

Device Networking: In a modern networked production, machine devices (e.g., PLCs) must be able to communicate to exchange data and information. In order to ensure a secure communication of machine tools, three strategies can be applied:

1. Secure Devices: Machine devices that are up to date in terms of security are allowed to communicate in the OT-network. This requires regular security updates and the use of secure communication protocols.
2. Edge Devices: Machine devices that are not up to date in terms of security should not be allowed to communicate in the OT network. If the devices offer any kind of connectivity option, an edge device can be installed between the unsecure machine device and the OT network. The edge device therefore takes over the communication in the OT-network and follows the security requirements.
3. Retrofitting: If a machine device does not offer any kind of connectivity, retrofitting the machine, e.g., by applying external sensors, can be used to extract information and securely connect the data from the sensors to the network.

Remote Access: Accessing machines from a remote service often helps to quickly contact the manufacturer of the machine for support. To prevent remote access from being misused by attackers, connections should only be allowed after a request is made within the organization. The connection itself should be established by a secure technology (e.g. VPN) and should only be temporary. Additional security can be achieved by not allowing remote access in the OT network. This can be achieved by creating a separate network withing the OT network which uses a mobile network access for the remote access service.

Detect

Even the best security protection measures cannot guarantee 100 percent protection. Therefore, it is essential to quickly detect ongoing attacks. For this purpose, the tracking of anomalies and events is crucial. Different kinds of Intrusion Detection Systems (IDS) can achieve this goal which are introduced in this chapter.

IDS are available under two different working principles: signature-based or anomaly-based detection measures. A signature-based detection uses the forensic information of previous cyber-attacks. Worldwide cyber-attacks are analyzed and characteristic information about the attack is stored in signatures. This information is used by the signature-based IDS to create an alarm as soon as a known signature is detected. This working principle helps to detect known attacks but fails to detect unknown attacks or attacks that managed to make changes to their attack. In these cases, anomaly-based detection can be used. Instead of focusing on known attacks, anomaly-based IDS try to distinguish between a normal and anormal state of communication in the OT network. At first the normal state must be defined, e.g., through machine learning algorithms. After that, the IDS analyses the OT network for anomalies. In case of anomaly, an event is generated. Although anomaly-based IDS can help to detect cyber-attacks, they are often prone to false-positive alarms.

Even tough security detection technologies help to identify security events, a security expert often needs to confirm that a generated event is a cyber-attack and not a false-positive alarm. Therefore, an event detection process needs to be installed to ensure that events are identified in a prompt manner and responsible parties are alerted in case of an actual cyber-attack.

Respond & recover

After a cyber-attack is confirmed, an immediate response is needed to mitigate the harm of the attack. Therefore, a proper response planning and communication should be installed in advance. This includes a documented process of tasks, responsibilities within an organization, and communication channels to internal stakeholders and/or external partners (e.g. security companies). These precautions help to quickly initiate mitigation actions that help to contain the attack.

The last step of the NIST Framework deals with recovering from a cyber-attack. Analogous to the respond phase, a documented process for recover planning should be implemented in advance to a cyber-attack. This includes the development and implementation of appropriate activates to plan for resilience and to restore any capabilities or services that were impaired due to a cyber-security event [49].

Summary & Outlook

The report provides a brief overview of a theoretical guideline on how to enable security in an operation technology (OT) environment of manufacturing companies. The complete guidebook is accessible online in the ICNAP Digital Services and can also be downloaded as a PDF.

The theoretical guideline on how to enable security in an operational technology (OT) environment of manufacturing is structured in a three-step process. First, the general Defense-in-Depth strategy is introduced to provide a basic understanding of a layered security approach at different levels of the organization. Second, the four application areas Process, Organization, People, and Technology are introduced to provide a structure to the different application areas on which security measures have an impact. Lastly, the NIST security framework and its five phases are introduced. In each phase a brief description of the most relevant tasks is given.

Security is a serious threat to manufacturing companies, and studies show that the level of security is often not sufficient [50]. This study should encourage manufacturing companies to start addressing security concerns and does provide guidance how to enable a secure networked adaptive production.

References

[43] "The State of Industrial Cybersecurity: Converging IT and OT with people, process, and technology. 2020 industrial cybersecurity survey report for IT and OT teams in the United States, Germany, and Japan.," Trend Micro Incorporated, 2021. Accessed: Mar. 6, 2023. [Online]. Available: https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html

[44] C. Singleton et al., "X-Force Threat Intelligence Index 2022," Armonk, NY, 2022. Accessed: Mar. 2, 2023. [Online]. Available: https://www.ibm.com/downloads/cas/ADLMYLAZ

[45] R. Kiesel et al. "Cybersecurity in Networked Production: White Paper."doi: 10.24406/ipt-n-633345.

[46] Bundesamt für Sicherheit in der Informationstechnik (BSI), Ed., "Die Lage der IT-Sicherheit in Deutschland 2021," Bonn, 2022. Accessed: Feb. 28, 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6

[47] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman, "Guide to Operational Technology (OT) Security: Initial Public Draft," 2022, doi: 10.6028/NIST.SP.800-82r3.ipd.

[48] National Institute of Standards and Technology (NIST). "Guide for conducting risk assessments: NIST SP 800-30 rev 1." doi: 10.6028/NIST.SP.800-30r1.

[49] A. Mahn, D. Topper, S. Quinn, and J. Marron, "Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide," Rep. 1271, 2021, doi: 10.6028/NIST.SP.1271.

[50] A. Kreppein, A. Kies, and R. H. Schmitt, "Novel Maturity Model for Cybersecurity Evaluation in Industry 4.0," in Advances in Cyber Security: Third International Conference, ACeS 2021 Penang, Malaysia, August 24–25, 2021. Revised Selected Papers (Communications in Computer and Information Science 1487), N. Abdullah, S. Manickam, and M. Anbar, Eds., Singapore: Springer Nature, 2021, pp. 198–210. doi: 10.1007/978-981-16-8059-5_12.