Repository of Hochschule Hannover

HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS

IT security in production facilities - An introduction to OT Security for small and medium-sized companies - 2nd completely revised edition

Karl-Heinz Niemann

Suggested citation:

Niemann, Karl-Heinz. 2025. "IT security in production facilities - An introduction to OT Security for small and medium-sized companies - 2nd completely revised edition." 2nd ed. Hannover: Hochschule Hannover. https://doi.org/10.25968/opus-4010.

Abstract

The first edition of this white paper dates to 2016. Many things have changed since then. For example, the term "OT Security" was established instead of "IT security in production facilities". This document still bears the title of the first version, as it is a new, updated edition. Nevertheless, the term "OT Security" will be used in the document. But more has happened. The IEC 62443 standard was created and is still being developed. Legislation has given planners, operators and manufacturers new tasks with new requirements such as the NIS2 Directive, CER Directive, Cyber Resilience Act and Machinery Regulation. Cyber incidents are becoming more frequent, including incidents in production. The term OT Security is emerging. Demographic change and changes in young people's study habits are creating gaps in project departments that are unlikely to be filled quickly.

This creates new challenges, especially for small and medium-sized enterprises (SMEs) to meet growing requirements in the face of an intensified threat situation and a shrinking workforce. This white paper is intended to support these companies in their daily work in OT Security and to show ways of adapting OT Security to the size of the company.

I am pleased to be able to present you with an updated version of the white paper after almost ten years. I would like to thank Wago GmbH & Co KG for their support in creating this document and for stimulating discussion and valuable comments on the drafts.

Terms of use **UrhG**

This document is made available under these conditions:
Urheberrechtlich geschützt
For more information see:
https://rightsstatements.org/page/InC/1.0/

IT security in production facilities

An introduction to OT Security for small and medium-sized companies

2nd completely revised edition

Prof. Dr. Karl-Heinz Niemann – University of Applied Sciences an Arts Hannover
in cooperation with Wago GmbH & Co.

Author:
Prof. Dr. Karl-Heinz Niemann
Email: Karl-Heinz.Niemann@Hs-Hannover.de
ORCID ID: https://orcid.org/0000-0001-8931-6789

DOI: https://doi.org/10.25968/opus-4010

© 2025 WAGO GmbH & Co. KG All rights reserved.

WAGO GmbH & Co. KG
Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 - 0
Fax: +49 (0) 571/8 87 - 1 69
E-mail: info@wago.com
Web: www.wago.com

Disclaimer: The information on which this document is based has been compiled with the greatest possible care. Nevertheless, it is provided without any guarantee. The author expressly rejects any kind of contractual or legal liability for this document. In no event shall the author be liable for any damages arising from errors or omissions in this document. Logos and brand names are used without reference to any existing property rights.

Foreword by the author

Dear reader

The first edition of this white paper dates to 2016 [NIE2017]. Many things have changed since then. For example, the term "OT Security " was established instead of "IT security in production facilities". This document still bears the title of the first version, as it is a new, updated edition. Nevertheless, the term "OT Security" will be used in the document. But more has happened. The IEC 62443 standard was created and is still being developed. Legislation has given planners, operators and manufacturers new tasks with new requirements such as the NIS2 Directive, CER Directive, Cyber Resilience Act and Machinery Regulation. Cyber incidents are becoming more frequent, including incidents in production. The term OT Security is emerging. Demographic change and changes in young people's study habits are creating gaps in project departments that are unlikely to be filled quickly.

This creates new challenges, especially for small and medium-sized enterprises (SMEs) to meet growing requirements in the face of an intensified threat situation and a shrinking workforce. This white paper is intended to support these companies in their daily work in OT Security and to show ways of adapting OT Security to the size of the company.

I am pleased to be able to present you with an updated version of the white paper after almost ten years. I would like to thank Wago GmbH & Co KG for their support in creating this document and for stimulating discussion and valuable comments on the drafts.

Hanover, September 2025

Table of contents

1. Introduction 6
2. The current state of OT Security 7
   2.1. Known security incidents in production facilities 7
   2.2. Future challenges for OT Security in production 9
   2.3. Fields of action in relation to OT Security in production systems 11
3. Norms , standards , guidelines 14
   3.1. Norms and standards for the office sector (IT security) 15
   3.2. Norms and standards for the production sector (OT Security) 16
      3.2.1. IEC 62443 Series of standards 16
      3.2.2. VDI/VDE standard series 2182 20
      3.2.3. VdS 10020 23
      3.2.4. Guidelines of the Federal Office for Information Security (BSI) 23
      3.2.5. Guidelines from manufacturer organizations 24
      3.2.6. Standards for the Maritime Sector 24
      3.2.7. Other industry-specific standards 25
      3.2.8. Summary of norms and standards 25
4. Legal requirements 27
   4.1. Requirements at EU level 27
      4.1.1. CER Directive 27
      4.1.2. NIS Directive 28
      4.1.3. NIS2 Directive 28
      4.1.4. Cyber Resilience Act 30
      4.1.5. Machinery Regulation 31
   4.2. National German requirements 32
      4.2.1. IT Security Act and BSI Criticality Ordinance 32
      4.2.2. KRITIS umbrella law 33
      4.2.3. NIS2 Implementation Act 33
5. Measures for the implementation of OT Security in production 34
   5.1. Management commitment 34
   5.2. Organization of responsibilities and processes 35
   5.3. Creation of guidelines 36
   5.4. Personnel 36
   5.5. Procurement and provision of knowledge 37
   5.6. Identification, assessment and protection of assets 38
   5.7. Regulation of external access to production facilities 42
   5.8. Data backup 44
   5.9. Handling faults and outages 46

5.10. OT Security - Detecting incidents 46
6. Outlook 48
7. List of figures 50
8. List of tables 51
9. Index 52
10. Bibliography 54

1. Introduction

When the first edition of this document was published nine years ago, the term "IT security in production plants" was chosen as the title. In the meantime, new terms such as cyber security, industrial security, ICS security and OT Security have become common. In this document, the term "OT Security" is used to clearly identify the area of application. OT refers to "Operational Technology ", which includes automation components and networks.

The target group of this document are small and medium-sized enterprises (SMEs) that are looking for a simple and scalable process model for ensuring OT Security in their production area.

To sensitize readers to the necessity of OT Security , chapter 2 presents security incidents that affected production facilities. It shows that cyber-attacks on production facilities are no longer a coincidence but are based on a targeted approach of the attackers. In addition, many incidents are also side effects of attacks on the company's IT that have spread into the production area.

This is followed in chapter 3 by an overview of the most important standards and recommendations on the topic of "OT Security ".

Chapter 5 uses a ten-step plan to develop a concept for setting up an OT Security system for small and medium-sized enterprises (SMEs). The focus is not only on the technical measures, but also on the often-neglected organizational measures.

Chapter 4 provides an overview of the requirements derived from EU and national legislation. In particular, the NIS 2 Directive, CER Directive, Cyber Resilience Act and Machinery Regulation should be mentioned here.

Finally, chapter 6 provides an outlook on future requirements and solutions in the context of vertical and horizontal integration.

2. The current state of OT Security

This chapter provides an overview of the current state of OT Security. Based on known security incidents, the challenges for current production facilities are derived. The top 10 threats of the Federal Office for Information Security (BSI) serve as the basis for this.

2.1. Known security incidents in production facilities

The requirements in terms of OT Security are constantly changing. In the past, IT security incidents in production were usually "collateral damages" from common malware attacks that emerged into a production facility by accident. One of the first known incidents of this kind was the attack on various Daimler Chrysler (now Mercedes Benz) plants in 2005 by the malware "Zotob" [PAK2005]. This affected 13 of the company's plants worldwide. The damage caused was estimated at US$ 14 million at the time [TOF2009].

Other incidents show that malware explicitly targeting production facilities is also increasingly being used. The most prominent case to date, "Stuxnet" [FAL2011] [LAN2013], targeted an Iranian uranium enrichment plant. The USA and Israel are named as the suspected perpetrators in this case [BRO2011]. Other incidents have also been documented that cannot be attributed to any state intervention. The German Federal Office for Information Security (BSI), for example, reports a dedicated attack on a blast furnace in Germany that led to its breakdown [BSI2014]. In addition, malware now exists that specifically attacks components of automation systems. The malware "Industroyer " [CHE2017] addresses industrial protocols such as:

- IEC 60870-5-101
- IEC 60870-5-104
- IEC 61850
- OLE for Process Control Data Access (OPC DA)

The ICS-CERT also reports malware that infects OPC servers [CERT2018]. In 2024, an attack on the Modbus protocol by the FrostyGoop group [GRA2024] was documented.

A new dimension of cyber-attacks on automation systems and critical infrastructure was marked by an attack on Ukraine's energy supply system on December 23, 2015 [CERT2016]. Three energy suppliers were attacked almost simultaneously, resulting in a power outage for 225,000 customers. During the attack, circuit breakers in the energy supply network were operated in an uncontrolled manner via remote access. At the same time, data was deleted from control computers so that they were no longer operational.

With the emergence of encryption Trojans such as WannaCry and Petya/NotPetya, ransomware has been a persistent problem for IT and OT systems since 2017

[SCH2018]. The example of the Colonial Pipeline in the USA [CYB2020] has shown that IT infections also spread to the OT. A cyber attacker used a spear phishing link, a scam email targeting a specific person, to first gain access to the company's IT network before switching to the OT network. The threat actor then used ransomware to encrypt data on both networks. Specific assets that suffered a loss of availability on the OT network included operating and monitoring stations (HMI), historical data logging servers and polling servers. Due to the loss of the operating function, the pipeline could no longer be operated and had to be shut down.

After the attack on the company SolarWinds in 2020 [ALK2021], the topic of "Security in the supply chain" became increasingly important. In this incident, attackers infiltrated the software development processes of the US company SolarWinds and incorporated malware called "Sunburst" into an update of the Orion network management platform. This update was delivered to 18,000 customers worldwide. The malware gave the attackers access to the customers' IT systems [ALK2021], [FOR2025]. In a study conducted by Ottorio [OTO2022], 53% of those surveyed saw a supply chain attack as the highest risk. The TÜV cybersecurity study [TÜV2025] states that in 10% of incidents, the attack was carried out via a customer or supplier. The VDMA addresses this topic "Supply Chain Security" via a corresponding sample requirement specification [VDM2023]. Further information on the topic of "Security in the supply chain " can also be found in [LEL2021].

In addition to industrial automation systems, building automation components are affected in the same way. In 2013, a case was documented in which heating systems were connected to the internet without adequate protection for the purpose of remote maintenance [EIK2013], [STA2013]. Due to a lack of protection, external individuals were able to gain access to these systems. Despite publication of the vulnerability in the trade press and rectification by the manufacturer, a large number of vulnerable heating systems were still accessible unprotected on the Internet two years later [STA2013]. Users did not install the security updates provided and the devices were still vulnerable. In a study from 2023, the authors Li et al. summarize the security situation in the field of building automation [LI2023] and report a series of cyber incidents in the field of building automation, as shown in Figure 1.

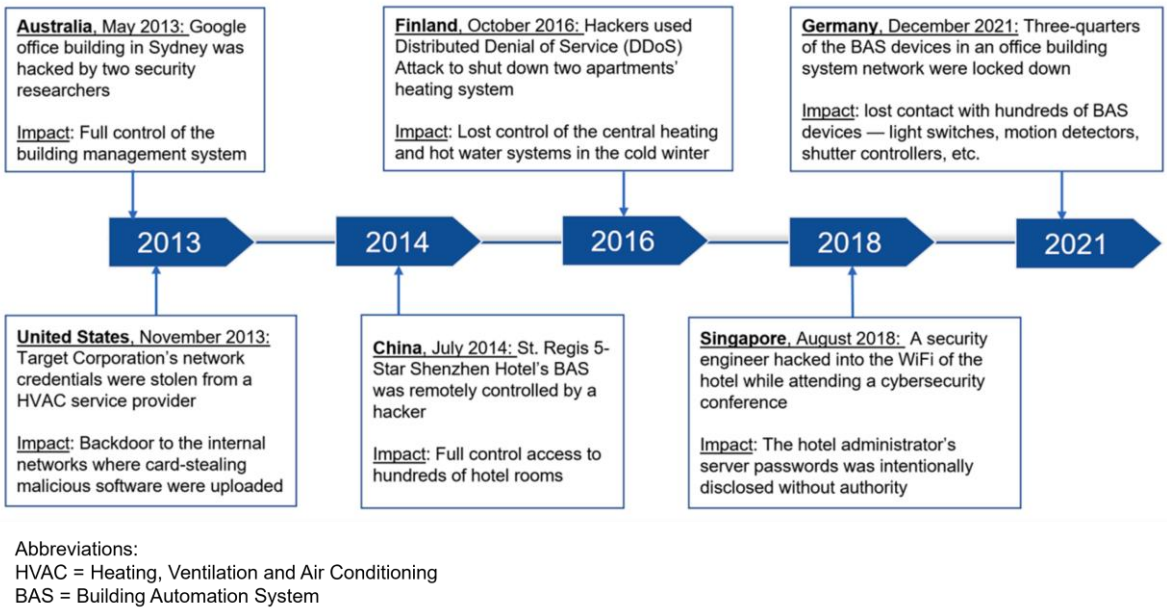

Figure 1: Cyber incidents from the building automation sector [LI2023]

It can be seen that building automation is a target for attackers. The German Federal Office for Information Security (BSI) has now addressed the topic of building automation as part of the BSI baseline protection and has published corresponding basic protection modules for technical building management [BSI_INF.13], [BSI_INF.13U] and building automation [BSI_INF.14], [BSI_INF.14U], which are available in the 2023 version.

The maritime sector must also face the challenges of cyber security. Although the automation systems used on ships are equipped and certified for this special purpose, they are generally based on conventional automation systems. This means that the same threats apply to these systems as to conventional automation systems [JEN2015]. Additional electronic systems for navigation and collision avoidance also increase the attack surface for potential attackers [DIR2015]. The "Maritime Cyber Attack Database" [NHL2025] provides a comprehensive overview of attacks in the maritime sector. The increasing challenges in the maritime sector are being met by corresponding standards in the context of classifying ships [UR_E26], [UR_E27].

Following this general overview, this document will deal with production systems in the process and manufacturing industries.

2.2. Future challenges for OT Security in production

It can be assumed that the future threat situation for automation systems will continue to intensify. This is indicated by the number and development of documented attacks over time. The increasing networking associated with the digitization of production processes to realize a horizontal and vertical integration of production processes will lead to further opportunities for attacks.

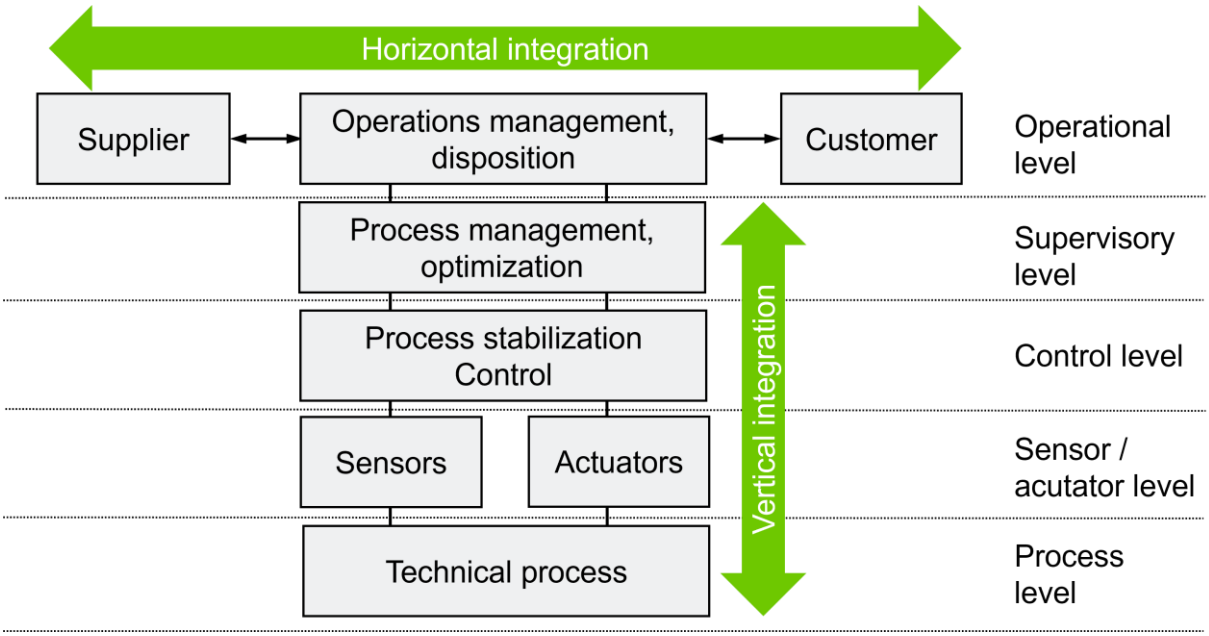

Figure 2: Horizontal and vertical integration

Figure 2 uses the example of a classic automation system to illustrate horizontal and vertical integration, which will be explained in more detail below:

Horizontal integration: This term describes the digital networking of supply chains that extend beyond company boundaries. This networking increases the attack surface of the companies involved, as data exchange, e.g. of quality data, can extend into the production area. In addition, the aspect of data sovereignty of the companies involved also plays a role. Concepts for "secure" data exchange in terms of OT Security while maintaining data sovereignty can be found, for example, in [KAL2024], [VOß2024] and [KAL2025].

Vertical integration: Vertical integration describes the increasing pervasiveness of industrial communication in the production sector. In the past, information that was generated or consumed at the measurement and control level was processed at the control level. In other words, only neighboring levels exchanged information with each other. As part of vertical integration, information from the measurement and control level is now also exchanged with the operating level or even with the cloud. This is the case, for example, when a sensor or actuator exchanges status information or maintenance requests with a computerized maintenance management system (CMMS). This type of communication is critical from the point of view of OT Security because the usual compartmentalization of levels no longer applies here. The protocols used for vertical communication, such as OPC-UA and MQTT, must be considered in terms of their security properties. See also [STE2019].

The German Federal Office for Information Security regularly publishes a list of the top 10 threats for automation systems. The current edition [BSI2022b] lists the threats listed in**Fehler! Verweisquelle konnte nicht gefunden werden.**Table 1.

Table 1: Top 10 threats [BSI2022b] extended by fields of action

Threat	Fields of action
Infiltration of malware via removable media and mobile systems	Human, processes
Infection with malware via internet and intranet	Processes, technology
Human error and sabotage	Human
Compromise of extranet and cloud components	Processes, network
Social engineering and phishing	Human, processes
(D)DoS attacks	Network, technology
Internet-connected control components	Technology
Intrusion via remote maintenance access	Network, technology
Technical malfunction and force majeure	Network, robustness
Software and hardware vulnerabilities in the supply chain	People, processes, technology

It can be seen that the top 10 threats mentioned can be assigned to different types of attacks and therefore different fields of action. Attacks can be carried out in different ways: E.g. via the network, via compromised components (USB sticks, smartphones) but also via social engineering or phishing. The overloading of components or networks through a flood of nonsensical requests (denial of service, distributed denial of service) is also a type of attack. Based on the threats described the fields of action for the implementation of an IT security concept for production facilities will now be derived in the next section.

2.3. Fields of action in relation to OT Security in production systems

To clarify the fields of action, the author has extended Table 1. Fields of action have been added the right-hand column. Individual topics can be assigned to one or more fields of action, which are briefly described below:

- **People:** People operate and monitor the production plant and are responsible for its security. At the same time, people represent a weak point in terms of OT Security . Via social engineering and phishing, they can unintentionally give third parties access to the system. In the event of misconduct or sabotage, people compromise the OT Security of the system either intentionally or unintentionally.
- **Technology**: The technology used (control components, network components) must be protected against attacks. Vulnerabilities that are known must be rectified promptly. Regular communication with the manufacturer of the components, e.g. by subscribing to security advisories, is advisable.
- **Processes**: Not all aspects of OT Security can be solved using technology. In many cases, appropriate processes (rules, regulations) must be defined alongside the technology. Employees must be regularly trained in these processes. Compliance with the processes must be monitored and any misconduct must be sanctioned. This point is therefore related to the "People" point.

- **Network**: Although the communication network of a production plant is assigned to technology, it is mentioned separately here. In many cases, the network is one of the main gateways for attacks. Special attention is required here to ensure that the production network is sufficiently separated from the rest of the company network and especially from the Internet.
- **Robustness:** Denial of Service (DOS) attacks or Distributed Denial of Service attacks (DDoS) are usually directed against a company via the Internet and initially hit the company's outer perimeter. Even if an attack to the production plant requires the penetration of further perimeters, automation systems must still have a certain robustness against overload situations.

The fields of action described show that OT Security is not an exclusively technical problem. In addition to technical problems (weak points in software, software patch not installed), weak points can also be caused by organizational inadequacies (employees do not know that certain things are not permitted, regulation of access to system components).

The following steps can be derived from this situation. The OT Security concept of a production plant must consider organizational and social aspects (human behavior, human error) in addition to the technical aspects and aspects of network communication. Only a structured and multi-level approach can guarantee optimum protection of the plant. To organize the necessary processes, an **I**nformation **S**ecurity **M**anagement **S**ystem (ISMS) must be established in the company. The ISMS covers both IT and OT. The required security processes are defined, documented, implemented and monitored in the ISMS.

The planning, implementation and long-term operation of an ISMS is no easy task, especially for small and medium-sized enterprises (SMEs). The know-how required to set one up is high. The resources in the company for this are usually scarce or do not have the necessary training in this specific area. This is why future concepts are required that also provide SMEs with cost-effective yet secure solutions. An example of the introduction of an ISMS in an SME is described in [PUL2024a].

[ISO_IEC_27001] describes the structure of an ISMS for companies, while [IEC_62443-2-1] also provides for an ISMS for the production area. [NIE2024b] shows how the combined use of both standards can lead to a simplification of processes and a uniform ISMS.

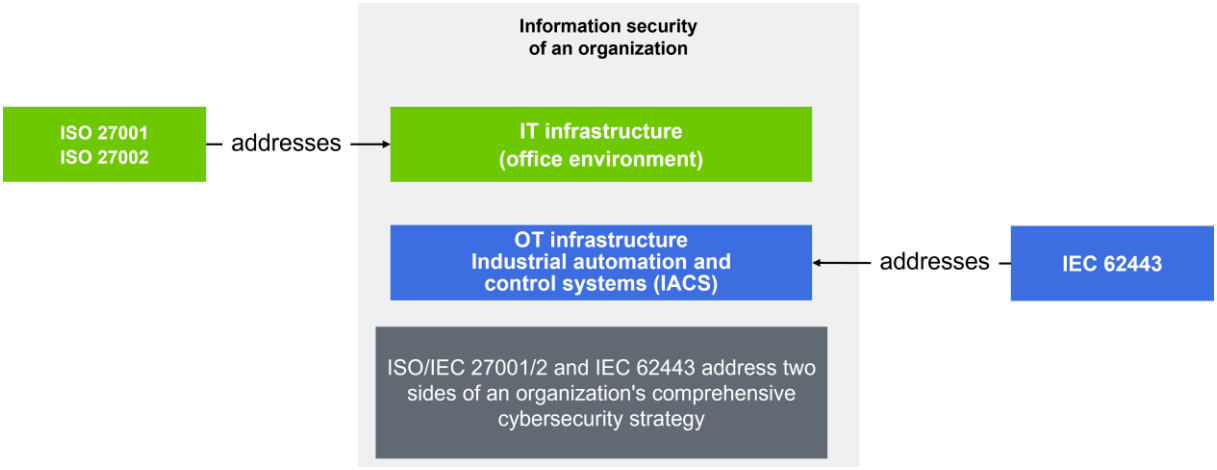

Figure 3: ISO 27001 / ISO 27002 and IEC 62443 as components of a cybersecurity strategy (based on [NIE2024b])

Figure 3 shows the relation between ISO 27001 and IEC 62443. ISO 27001 addresses the information security of an organization in general. The essential processes for setting up an ISMS can be established within the framework of this standard. This can also include the ISMS component for the production area. IEC 62443 then additionally covers the specific aspects for automation systems that are not included in ISO 27001. A detailed consideration of the combined use of both standards can be found in [NIE2021] and [KOB2021]. The two documents were created independently of each other but come to the same conclusions. Subsequently, the two authors decided to write a joint, consolidated article [NIE2024b] on this topic.

3. Norms , standards , guidelines

In the area of OT Security , companies have a number of standards and guidelines at their disposal. Standards are based on current knowledge and recognized rules. They enable a standardized approach to the design, implementation, operation and certification of OT Security systems.

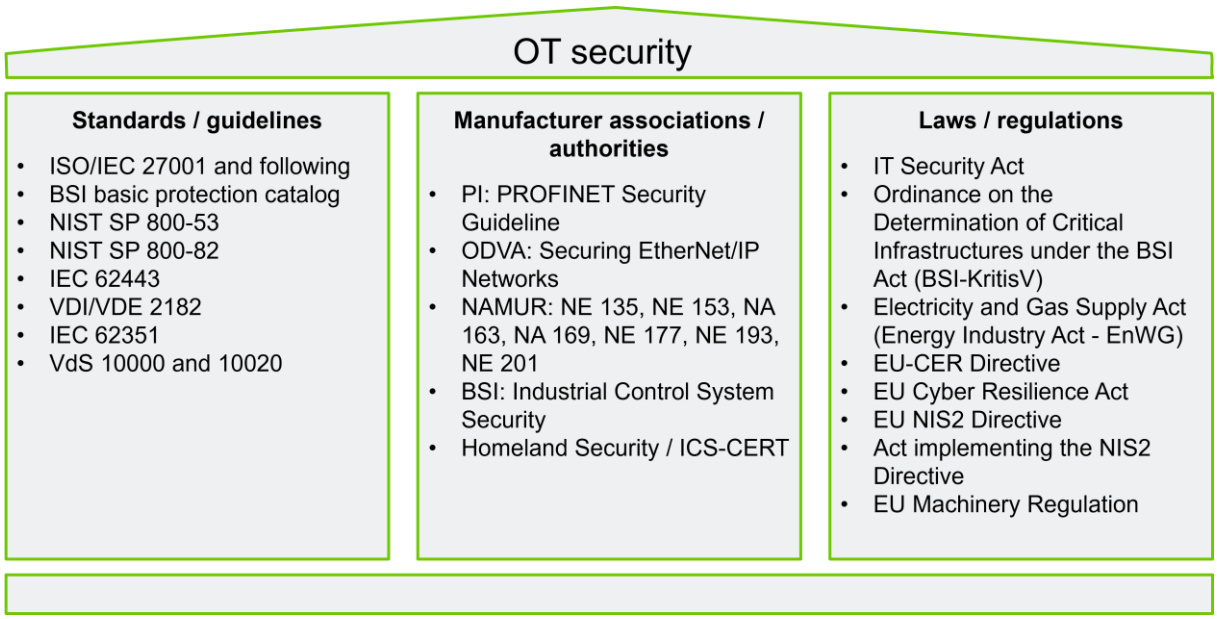

Figure 4: Overview of norms and standards for OT Security

Figure 4 provides an overview of norms and standards relating to OT security. In addition to norms and standards for the office area (ISO 27000 series, BSI basic protection catalog), which are required for the development of an ISMS , standards are also listed that specifically address the production area, i.e. OT Security . These include, for example, IEC 62443, IEC 62351 , NIST SP 800-82 , VDI/VDE 2182 , VdS 10000 in conjunction with VdS 10020 . The list is supplemented by a series of security recommendations from manufacturer/user associations such as PROFIBUS & PROFINET International for PROFINET , ODVA for EtherNet/IP and the interest group for automation technology in the process industry (NAMUR) as well as guidelines from authorities such as the Federal Office for Information Security (BSI) and the ICS-CERT of Homeland Security. The laws and regulations at EU and German level are listed on the far right of the drawing.

The following sections provide an overview of the available literature. The general standards for IT security (information security / IT security) are considered first. This is followed by an overview of special standards for automation technology (OT Security) and recommendations from manufacturer organizations. This is followed in chapter 4 by an outlook on the legal regulations at EU level and in Germany.

3.1. Norms and standards for the office sector (IT security)

The ISO 27000 series of standards deals with information security and the establishment of an information security management system (ISMS). An introduction can be found in [BRE2024]. The ISO 27000 series provides a comprehensive set of standards which, in addition to the organizational aspects, also describe the associated processes, implementation and certification. The series of standards begins with [ISO_27000], which provides an introduction and explains the terminology. This is followed by [ISO_IEC_27001]. This describes the structure of an ISMS and the risk-based approach. The required security measures are described in the appendix. The standard [ISO_IEC_27002] defines specific measures for implementation. There are several other standards. The website [ISE2025] provides a brief overview of all parts of the standard.

ISO 27000 management systems can be certified in accordance with the requirements of [ISO/IEC_27006-1]. The certification procedure can be found, for example, in [BRE2024], [HÄU2023]. The certification of an information security management system (ISMS) in accordance with the ISO 27000 series of standards is still not very widespread. Figure 5 shows the number of valid ISO 27001 certificates in Germany.

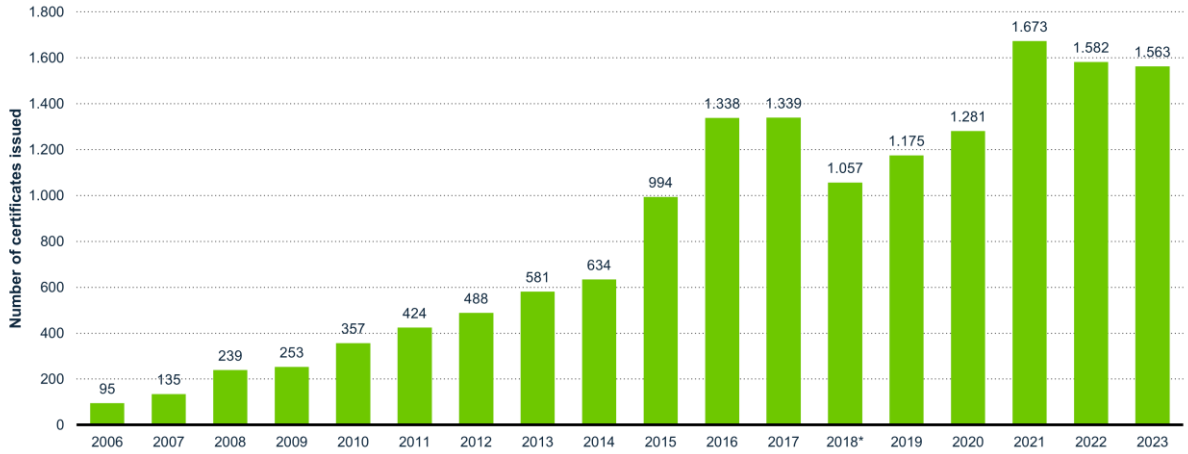

Figure 5: Number of valid ISO 27001 certificates in Germany in the years 2006 to 2023 [STA2025a]

The statistics provides a figure of 1,563 valid ISO 270001 certificates for the year 2023 [STA2025b]. This can now be put in relation to the number of companies in Germany. In 2023, this was a number of 3.1 million [STA2025a]. It can therefore be assumed that mainly companies that are considered particularly exposed (banks, payment service providers) are certified.

Based on the ISO 27000 series of standards, the German Federal Office for Information Security has defined a series of basic protection catalogs that provide simplified access to information security. The IT baseline protection compendium [BSI2023a] provides a good overview. The BSI also provides suitable checklists and survey forms. This allows SMEs easier access to the topic of IT security.

With the guidelines [VDS_10000], the VdS offers a guidance for cyber security in the office sector for SMEs, which is tailored to the needs of small and medium-sized enterprises. Certification according to this standard is possible. The effort involved is tailored to the needs of SMEs and is significantly lower than certification in accordance with the ISO 27000 series of standards.

3.2. Norms and standards for the production sector (OT Security)

The standards described in the chapter 3.1 address information security / IT security in the office area. This refers to the IT of a company that does not have any production facilities (e.g. banks) or the part of a company in which no production facilities are located (e.g. administration, sales, HR department, etc.). The requirements in the office area are prioritized as follows: Confidentiality, integrity and availability. Figure 6 shows the prioritization of these protection goals for the office area on the left-hand side.

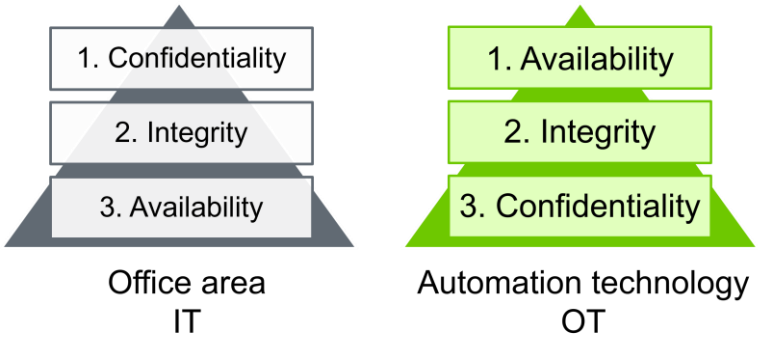

Figure 6: Prioritization protection goals for the office area (IT) and automation technology (OT)

Prioritization is different in the production area. As can be seen in Figure 6 on the right-hand side, the availability of the production system has the highest priority here, followed by the integrity of the system. Confidentiality is only in third place. The relatively low importance of confidentiality according to Figure 6 is due to the fact that the IO data communicated via a PROFINET , for example, contains very little information for an attacker. For this reason, PROFIBUS & PROFINET International (PI) differentiates the security function of PROFINET into different security classes [NIE2023a]. Class 2 includes integrity and authenticity, while class 3 also includes confidentiality. Depending on the risk assessment of the system operator, class 2 or class 3 can be used.

Due to this prioritization and due to the real-time behavior required for production systems in many areas, the standards described in chapter 3.1 are not applicable to the production area, or only to a limited extent. For this reason, several standards are being developed that consider the requirements of production. The following sections present the most important of these standards.

3.2.1. IEC 62443 Series of standards

The IEC 62443 series of standards is being developed by the International Electrotechnical Commission (IEC) and the International Society of Automation (ISA). The

initial work on the standard was started in the ISA 99 working group and is currently being continued in cooperation between the IEC and ISA. As a result, references to ISA working groups and documents can still be found in many documents.

The IEC 62443 series of standards considers the special requirements of OT Security in the production sector. Figure 7 shows the structure of the series of standards. The parts marked in green have already been published, the parts marked in gray are still being drafted and are not yet generally available.

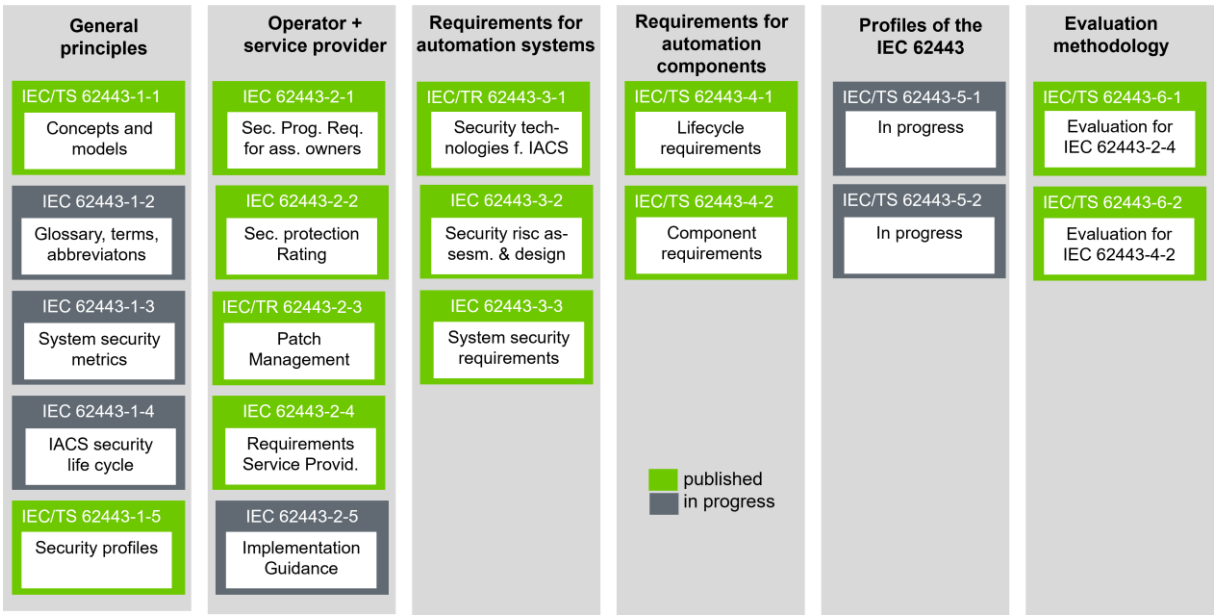

Figure 7: Parts of IEC 62443

The IEC 62443 series of standards consists of six main areas, which are presented below, including the associated standards:

In the **"General principles"** part, terms, concepts and models are first defined in [IEC_62443-1-1]. Part [IEC_62443-1-2] defines all terms used in the standards. Part [IEC_62443-1-3] defines metrics for the evaluation of OT Security , part [IEC_62443-1-4] describes the security lifecycle and use cases. The standard part [IEC_62443-1-5] describes the possibility of creating a profile by selecting selected parts of the standard.

The part **"Operator and Service Provider"** describes the information security management system (ISMS) and thus defines the organization of OT Security , followed by implementation aids. The part [IEC_62443-2-1] describes requirements for an information security management system (ISMS), e.g. the definition of security processes. The part [IEC_62443-2-2] provides information on how and in which areas these processes are to be implemented. Updating the software of automation systems, i.e. patching, is of particular importance because improper procedures can lead to malfunctions. The standard therefore devotes a separate part to patch management [IEC_TR_62443-2-3]. The part [IEC_62443-2-4] deals with the use of service providers for commissioning and service from an IT security perspective and defines requirements for these service providers.

The "Requirements for automation systems" section describes the procedure for planning a system and the OT Security requirements for a system. Part [IEC_62443-3-1] first describes the underlying technologies such as authentication, encryption, filtering and logging. Part [IEC_62443-3-2] describes the procedure for planning the security of a system, carrying out a risk analysis, defining the required security level (SL-T) and structuring a system into zones (isolated areas) and conduits (secure connections between the areas). This is intended to divide an automation system into subareas, which in turn are sealed off from each other. Figure 8 shows the risk analysis process in accordance with [IEC_62443-3-2]. The analysis first examines a zone or conduit in an initial analysis. If the initial risk exceeds a limit value to be defined by the company for the system, risk reduction measures have to be defined. This continues until the existing risk no longer exceeds the residual risk.

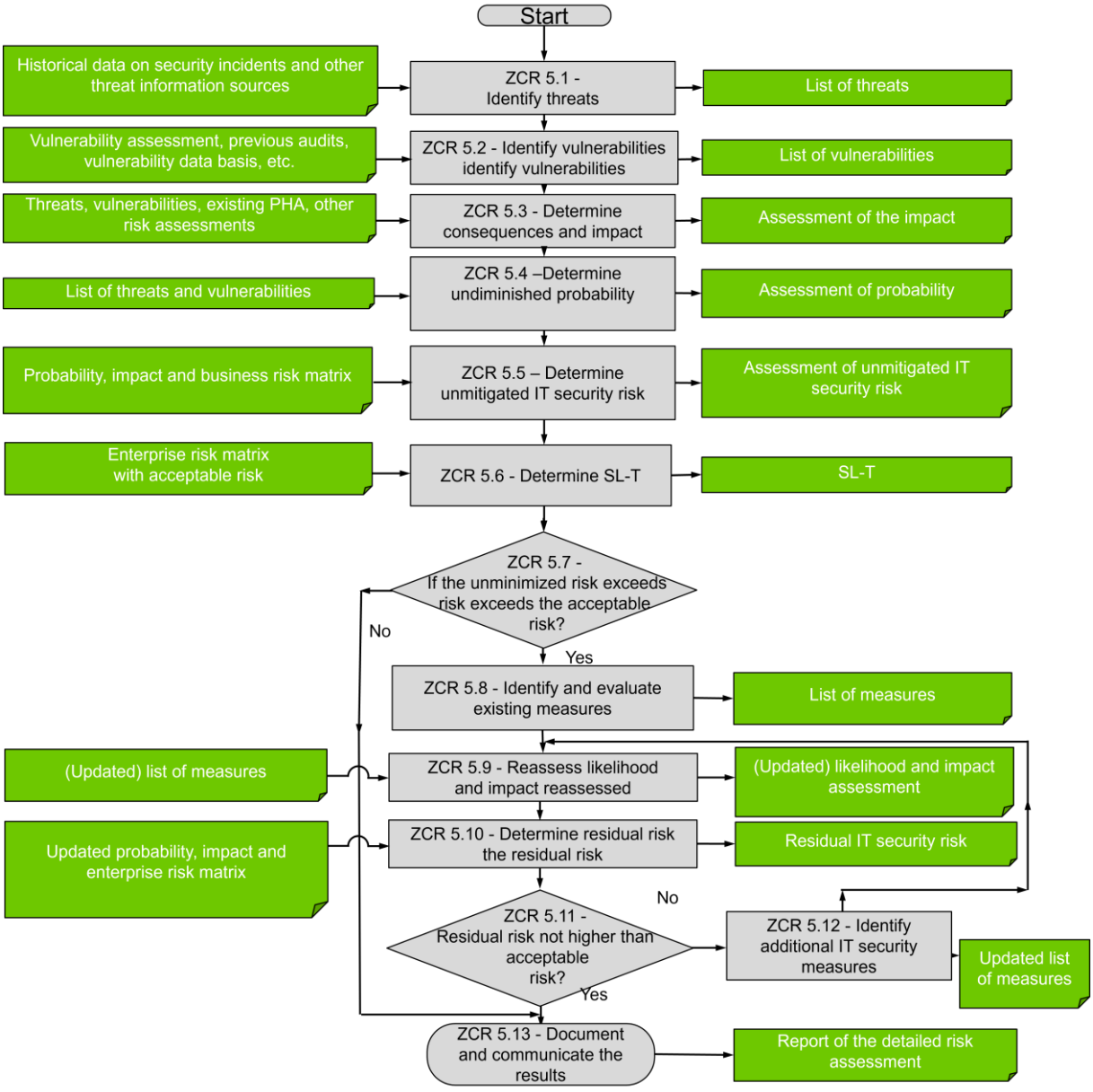

Figure 8: Risk analysis derived from [IEC_62443-3-2]

Part [IEC_62443-3-3] defines the security requirements for a system. This is based on the so-called "Foundational Requirements"):

- Identification and authentication control (IAC)
  - Registration of all users (human, software, component).
- Use contol (UC)
  - Enforcement of user access authorizations.
  - Recording of event data (logging).
- System integrity (SI)
  - Preventing manipulation of the IACS.
- Data confidentiality (DC)
  - Securing data in communication channels and storage.
- Restricted data flow (RDF)
  - Zone division and protected communication channels.
- Timely response to events (TRE)
  - Fast notification of entities about IT security incidents.
  - Event monitoring and logging
- Resource availability (RA)
  - Ensuring the availability of resources.
  - Protection against DoS attacks
  - Backup
  - Emergency power

The requirements are defined in a level between 1 and 4 according to the security level. As the security level increases, so does the severity of the requirement.

The section **"Requirements for automation components"** describes the requirements for components and the associated Secure Development Lifecycle (SDL). This part is aimed at manufacturers of automation systems. The part [IEC_62443-4-1] defines the development process that must be observed when developing components for automation technology. Topics such as: "Development process", "Specification of OT Security requirements", "IT security by design" and "Risk analysis and threat model" are part of the standard. The part [IEC_62443-4-2] describes the technical requirements for the components of automation systems, applications and functions. The paper [NIE2023b] uses the example of a PROFINET device to describe how the "secure" development of an automation component is carried out in accordance with the two parts of the standard described above.

The **evaluation methodology** part was published at the beginning of 2025. The standard [IEC_62443-6-1] describes criteria for evaluating the requirements of the standard [IEC_62443-2-4]. The part [IEC_62443-6-2] defines criteria for evaluating the requirements of the standard [IEC_62443-4-2].

The standards and draft standards published to date currently comprise 1,216 printed pages (as of September 2025). For a first insight into the standard, the "Guideline Industrial Security" [KOB2023] is recommended. The document provides an overview of the IEC 62443 series of standards and explains the relationships between the parts of the standard.

The IEC 62443 series of standards addresses the roles of operator (asset owner), planner (system integrator) and manufacturer. Parts of the series of standards are assigned to each of these roles. Figure 9 shows the interaction between the three roles described and the assignment of the parts of the standard.

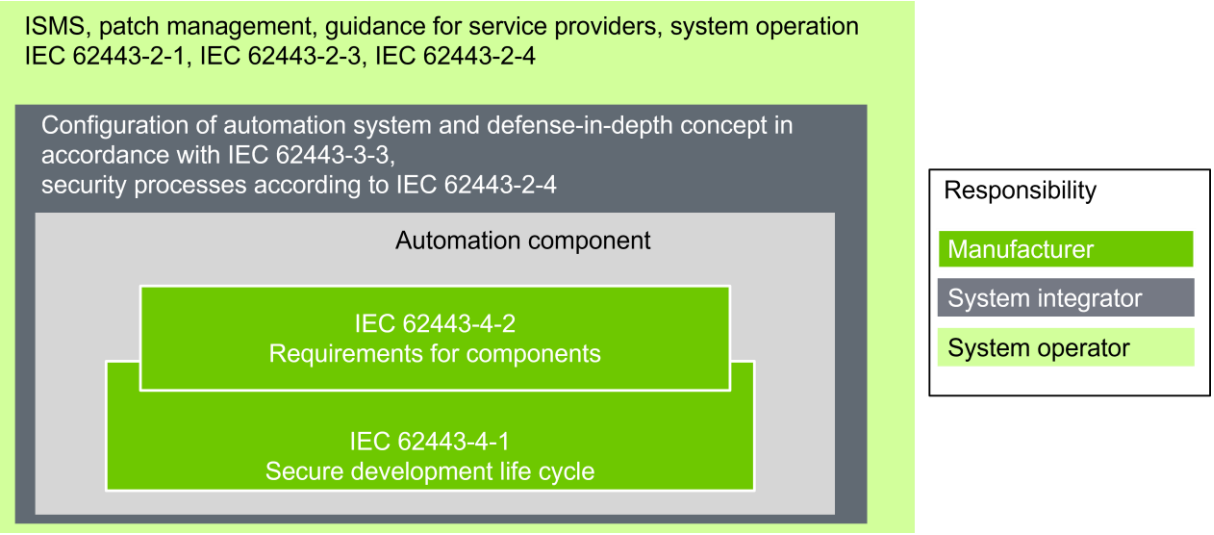

Figure 9: Responsibilities and associated standard parts in the security process

It can be stated that the IEC 62443 series of standards is the essential and most important standard for OT Security .

3.2.2. VDI/VDE standard series 2182

The VDI/VDE 2182 series of standards illustrates the topic of OT Security using specific examples for the manufacturing and process industries. The focus is on risk analysis in the OT sector. The views of manufacturers, integrators and operators are addressed. As an alternative to the procedure according to VDI/VDE 2182, the risk analysis can also be carried out according to the standard [IEC_62443-3-2]. This standard has a comparable approach and defines the process of safe system design and risk analysis. See the description in chapter 3.2.1

Part 1 of the standard [VDI_2182_1_en] first defines the key terms of OT Security:

- User
  - Person or application that can interact with the object under consideration.
- Asset
  - All tangible and intangible values of automation devices, automation systems, machines or production facilities that may be threatened and that are worth protecting
  - Examples: PLC, recipe, interface functions, firmware.
- Threat
  - A circumstance or event that can cause damage.
- Risk
  - Combination of probability and extent of damage.
- Risk reduction

    - Reduction of the probability of damage or the extent of damage through the application of protective measures.
- Vulnerability
    - Defect that allows a threat to become effective for the object under consideration.
- Originator
    - Authorized or non-authorized user whose actions can have intended or unintended negative effects on the protection objectives of an object under consideration.

The standard then defines a process model with associated roles, as shown in**Fehler! Verweisquelle konnte nicht gefunden werden.** Figure 10.

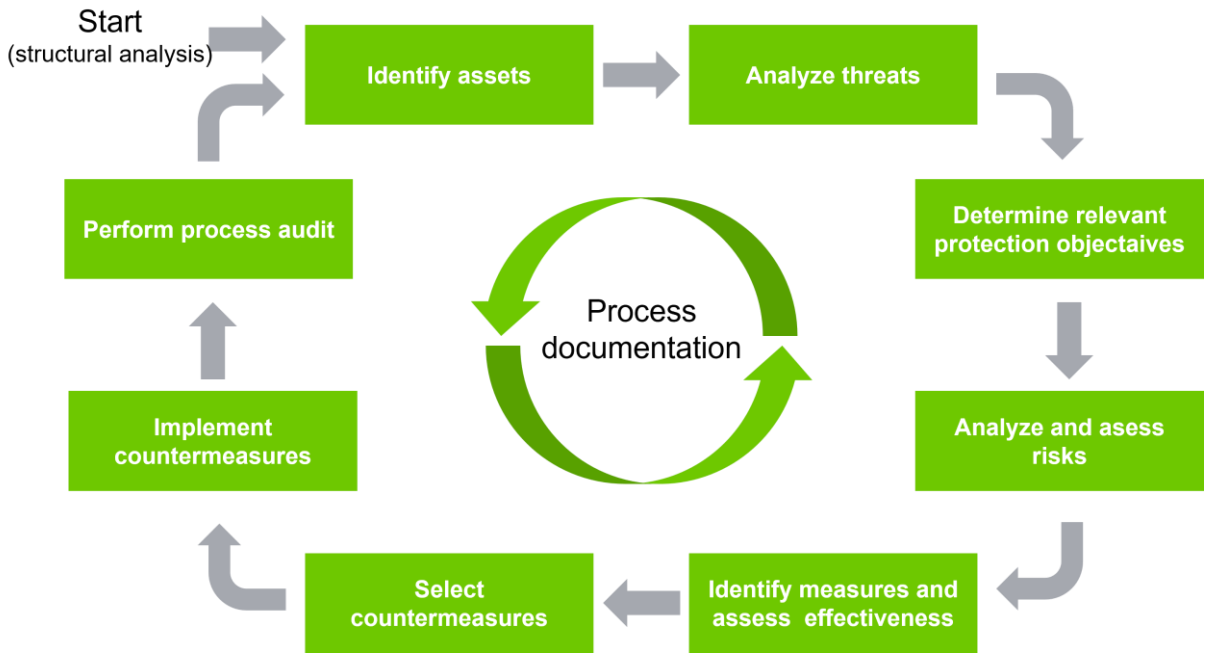

Figure 10: Process model according to [VDI_2182_1_en]

The VDI/VDE 2182 process model is based on a so-called "Plan-Do-Check-Act cycle" (PDCA).

1. The first step is to identify and record the assets of the system, in particular automation components, computers, servers, etc.). The result is a list of the identified assets.
2. The next step in the cycle is to identify the threats that affect the assets. Threat scenarios are considered and documented. The [VDI_2182_1_en] provides corresponding templates.
3. In the third step, the standard provides for the determination of the relevant protection goals. Derived from the threats, the protection goals are defined and documented for each asset.
4. The fourth step of the process model now provides for a risk assessment. Based on the threats and the identified protection goals, the probability of the identified threats occurring and the associated potential damage are described. An

assigned risk can be identified from the combination of probability of occurrence and level of damage.

5. The result of the risk assessment identifies areas in which the existing risk is unacceptable. Here, measures to reduce the risk, known as protective measures, must be provided and evaluated in terms of their effectiveness and cost-effectiveness.
6. Based on the considerations from step 5, the protective measures are now selected. The aim of this selection is to implement protective measures within an economically justifiable framework and at the same time achieve the required risk reduction.
7. The next step involves implementing the selected protective measures.
8. Based on the previous steps, an audit of the described process is then carried out. This determines the documents created and the effectiveness of the protective measures described. The audit should be carried out by people who were not involved in the previous steps.

As the threat situation for a production facility can change due to external events, this process should be repeated at certain intervals. The same applies in the event of changes or extensions to the plant.

To support the process described, software tools are available that support the recording and evaluation of assets. For example, the Federal Office for Information Security provides the LARS tool [BSI2025]. Homeland Security offers the tool CSET [ICS2025]. Both tools focus on OT Security. The "Microsoft Threat Modeling Tool " is also known from the IT sector [MIC2023]. This tool uses the STRIDE approach for analysis. STRIDE describes possible attack vectors, which are described in more detail in**Fehler! Verweisquelle konnte nicht gefunden werden.**Table 2.

Table 2: Meaning of the abbreviation STRIDE

Abbreviation	Meaning	Description
S	Spoofing	An attacker pretends to be someone else (identity theft).
T	Tampering	Unauthorized modification of data or code.
R	Repudiation	The ability to deny an action, e.g. a transaction.
I	Information Disclosure	Unauthorized access to confidential information.
D	Denial of Service	Attacks that restrict or prevent the availability of a system.
E	Elevation of Privilege	An attacker obtains higher rights than intended.

The VDI/VDE 2182 series of standards defines the risk analysis process in relation to three roles:

- **Manufacturer** : The manufacturers develop and distribute the system components. They are also responsible for the maintenance and servicing of the supplied components (e.g. software updates to eliminate security vulnerabilities).
- **Integrator** : The integrator is a service provider commissioned by the operator who is responsible for the planning and commissioning of a system. System operators often do not have sufficient resources to plan and commission new

systems or to carry out system modifications. The use of integrators is therefore a common practice.
- **Operator** : The operator (asset owner) is responsible for the operation and maintenance of the system. The operator may delegate maintenance tasks to maintenance service providers.

Parts 2 and 3 of VDI/VDE 2182 follow the described role concept. Part 2 describes the tasks for the roles of manufacturer [VDI_2182_2_1_en], integrator [VDI_2182_2_2_en] and operator [VDI_2182_2_3_en] in accordance with the process model described in Part 1, using the example of a production plant in the field of manufacturing automation. The same can be found in Part 3 for a process automation system in the same way [VDI_2182_3_1_en], [VDI_2182_3_2_en], [VDI_2182_3_3_en].

The VDI/VDE 2182 series of standards provides manufacturers, integrators and operators with a basis for structured risk analysis. The document offers a view of the PDCA procedure model that focuses on the respective responsibilities. The respective sections use a real example to guide the reader through the process and provide checklists to show how the results can be documented.

3.2.3. VdS 10020

The [VDS_10020] targets at small and medium-sized enterprises (SMEs) and is a supplement to the existing guideline [VDS_10000]. The VdS 10020 focuses on SMEs that operate production facilities. The criteria required for the implementation of an OT Security strategy in the production sector are described in a concise and clear form.

3.2.4. Guidelines of the Federal Office for Information Security (BSI)

The German Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik BSI) offers a series of guidelines in the area of OT Security. Traditionally, the BSI refers to automation systems as ICS (Industrial Control System). For this reason, the term ICS security is often used in BSI documents.

At regular intervals, the BSI publishes the top 10 threats for automation systems and the associated countermeasures [BSI2022b]. In addition, the BSI offers an introduction to OT Security for system operators in the form of the ICS security compendium [BSI2024]. The document "Requirements for network-enabled industrial components" [BSI2018a] is aimed at manufacturers of automation components and defines requirements for automation system components. In addition to these basic documents, the BSI publishes case studies at regular intervals in which specific aspects are addressed. For example, there are case studies of a possible attack on a public swimming pool [BSI2018c] through the use of hard-coded passwords and an example of a service technician who unknowingly introduced malware into a system via a contaminated USB stick [BSI2018b].

The topic of remote service and remote diagnostics is of particular importance, as communication connections from the automation sector are operated via the Internet to third parties. The BSI dedicates a separate module to this topic in the BSI baseline protection [BSI2022a].

3.2.5. Guidelines from manufacturer organizations

Industrial communication systems such as PROFINET or EtherNet/IP are an important part of an automation infrastructure. For this reason, the various manufacturing organizations have addressed the topic of OT Security and published corresponding guidelines.

For example, PROFIBUS & PROFINET International (PI) offers a guideline for planning PROFINET [PNO2013] taking OT Security into account . This guideline is currently being revised and will be published in the foreseeable future. In addition, PI has developed a security concept that enables cryptographic protection of PROFINET communication. Various guidelines and publications have already appeared in this regard. These include, for example

- Security extensions for PROINET [PNO2019].
- OT Security for production systems with PROFINET . A classification of IEC 62443 for operators, integrators and manufacturers [PNO2022].
- Security event logging using the example of PROFINET [NIE2024a].
- Security Class 1 for PROFINET -Security Guideline for PROFINET [PNO2023].
- How to develop a secure PROFINET device. Organizational and technical OT Security measures in the development of PROFINET devices [NIE2023b].
- Security Extensions for PROFINET. Concepts, Status, and Prospects [NIE2023a].

Comparable documents are available from ODVA under the name "CIP-Security " for EtherNet/IP [ODV2023], [VIS2020]. Furthermore, a security model for OPC UA is available as an IEC Technical Report [IEC_62451-2]. The German Federal Office for Information Security has evaluated this concept and essentially assessed it positively [BSI2022e].

3.2.6. Standards for the Maritime Sector

Internationally, the International Maritime Organization (IMO) sets the regulatory framework for OT Security on ships. Resolution MSC.428(98) [IMO2017] is a central document. It requires cyber risks to be systematically considered in safety management by the first annual review of the Document of Compliance after 1st January 2021 at the latest. In addition, the IMO guidelines on maritime cyber risk management MSC-FAL.1/Circ.3/Rev.3 [IMO2025] provide support for risk assessment, protective measures, detection, response and recovery.

For ships, the International Association of Classification Societies (IACS) created the IACS Unified Requirements E26 (Cyber Resilience of Ships) [UR_E26] and E27 (Cyber Resilience of On-Board Systems and equipment) [UR_E27] as binding minimum requirements for newbuilds. Among other things, they address the segmentation and hardening of on-board networks, the management of privileged access and remote maintenance , patch and vulnerability management, logging and event detection as well as life cycle requirements for suppliers and integrators.

Classification societies have established their own notations and guidelines based on the above-mentioned standards (e.g. DNV Cyber Secure Class Notation [DNV2025], ABS CyberSafety [ABS2025], Lloyd's Register ShipRight Cyber [LLO2024]), some of which go beyond the UR and define test and acceptance criteria.

3.2.7. Other industry-specific standards

In addition to the manufacturers' associations, user associations also deal with the topic of OT Security . The interest group for automation technology in the process industry (NAMUR) published its first recommendation on OT Security back in 2006. Further documents have been published over the years. The most important documents are

- IT security for automation technology systems [NA_115_en].
- Remote maintenance for automation technology systems in the process industry [NE_135_en].
- Automation Security 2020 - Design, implementation and operation of industrial automation systems [NE_153_en].
- Automation Security Management in the process industry [NA_169_en].
- NAMUR Open Architecture - NOA-Security-Zones and NOA-Security-Gateway [NE_177].
- An information model for automation security engineering [NE_193].
- IT risk assessment of PLT security devices [NA_163_en].
- Identity and Access Management on Automation Devices [NE_201_en].

At this point, only a limited overview of industry-specific standards can be provided, which is not exhaustive.

3.2.8. Summary of norms and standards

Many of the documents described above are based on the "Plan-Do-Check-Act cycle" (PDCA cycle). In a structured procedure, assets are recorded, threats are identified, risks are assessed and the necessary measures are derived, implemented and verified, as described in the chapter 3.2.2 . Another common criterion is the establishment of an IT security strategy within the company, which requires a holistic and comprehensive approach. In addition to technical aspects, organizational and personnel aspects must also be considered.

In terms of technical implementation, the existing standards are based on a defense-in-depth strategy. A series of complementary measures are used to protect assets from external threats.

With increasing horizontal and vertical integration in the context of Industry 4.0, the existing concepts will have to be expanded and improved. In [NIE2014a], [NIE2014b] a number of additional challenges were defined back in 2014 that need to be addressed with regard to OT Security . These are in particular

- Protection against internal perpetrators
- Communication across company boundaries
- Access control to the network

- Securing communication with cryptographic means.

These challenges still apply today - 11 years later. Chapter 6 will take up and discuss these aspects once again.

4. Legal requirements

The topic of IT security and OT Security has gained in importance both at EU level and at national, German level. A separate main chapter is therefore devoted to this topic. The terms CER Directive , NIS2 Directive , Cyber Resilience Act (CRA) and the German IT-Sicherheitsgesetz are certainly familiar to many readers by now. For this reason, the legal requirements at EU level are dealt with in chapter 4.1, followed by the national German requirements in chapter 4.1.1.

!	The facts described in the following chapters regarding the legal requirements are currently still changing considerably. Much of the information on implementation is still being developed. The information provided here relates to the month of September 2025 and should be regarded as provisional. The circumstances will continue to change thereafter.

4.1. Requirements at EU level

In recent years, the European Union has addressed the issue of IT security, OT Security and resilience in the form of various directives. These include, for example Cyber Resilience Act (CRA), CER Directive, NIS Directive, NIS 2 Directive, Cyber Security Act, Machinery Regulation. The following chapters provide an overview of the parts relevant to OT Security. It should be noted that some of the requirements (e.g. CRA, Machinery Regulation) are directly legally binding. Others still need to be adopted into national law by the member states (e.g. CER Directive, NIS 2 Directive).

4.1.1. CER Directive

The EU's CER Directive (Critical Entities Resilience Directive, EU 2022/2557) [CER_en] was introduced to strengthen the physical resilience of critical infrastructure to threats such as natural disasters, sabotage or terrorist attacks. The abbreviation CER stands for "Critical Entities Resilience". It replaces the previous Directive 2008/114/EC on critical infrastructure from 2008 and obliges member states to identify operators of so-called "critical facilities" and improve their resilience through specific measures. These include risk analyses, protection concepts, crisis response plans and reporting obligations in the event of incidents. The directive covers eleven key sectors, including energy, transport, health, drinking water, digital infrastructure and public administration. The aim is to ensure security of supply and the functioning of society even in crisis situations.

The member states must transpose the directive into national law by October 2024; in Germany, this is done via the “Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen" (English translation: “Act on the Implementation of Directive (EU) 2022/2557 and on Strengthening the Resilience of Critical Installations") [BMI2024], the so-called “KRITIS Dachgesetz”. The transfer of

the CER Directive into the KRITIS Dachgesetz has not yet been completed (as of September 2025). A government draft has been available since November 2024 and has already been discussed in the Bundestag, but due to the break-up of the coalition, the legislative plans were not finalized before the new elections. This means that the draft must be reintroduced and discussed in the Bundestag. An updated draft bill was published on August 27, 2025 [BMI2025] and adopted by the Federal Cabinet on September 10, 2025.

4.1.2. NIS Directive

The NIS Directive 2016/1148 [NIS1_en] of the European Parliament and of the Council was created to ensure a "high common level of security of network and information systems in the EU". It was the first Europe-wide regulation on cybersecurity and laid the foundation for a coordinated security strategy for the member states. The aim was to strengthen the resilience of critical digital infrastructures and improve cooperation between EU member states. The Directive required member states to develop national cybersecurity strategies, set up single points of contact and computer security incident response teams (CSIRTs) and identify operators of essential services and certain digital service providers. These companies had to take security measures and report significant security incidents. The NIS Directive 2016/1148 was transposed into national law in Germany by the „Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148“ (englisch:"Act Implementing Directive (EU) 2016/1148") [BUN2017] of June 23, 2017. This law (colloquially known as the NIS-UG) amended the BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) (english: BSI Act (Act on the Federal Office for Information Security)) in particular and added regulations for operators of critical infrastructures and providers of digital services.

The NIS Directive was replaced by the NIS 2 Directive in 2022. See the following chapter 4.1.3.

4.1.3. NIS2 Directive

The NIS2 Directive (EU 2022/2555) [NIS2_en] has been in force in the EU since the beginning of 2023. It is the European framework for operators of critical infrastructures and defines minimum cyber security standards in the EU. NIS2 significantly extends the scope and obligations for companies. Essentially, the following changes are relevant:

Sectors : The critical Essential Entities increase to eleven sectors, the Important Entities grow to seven sectors - to a total of eighteen NIS2 sectors.

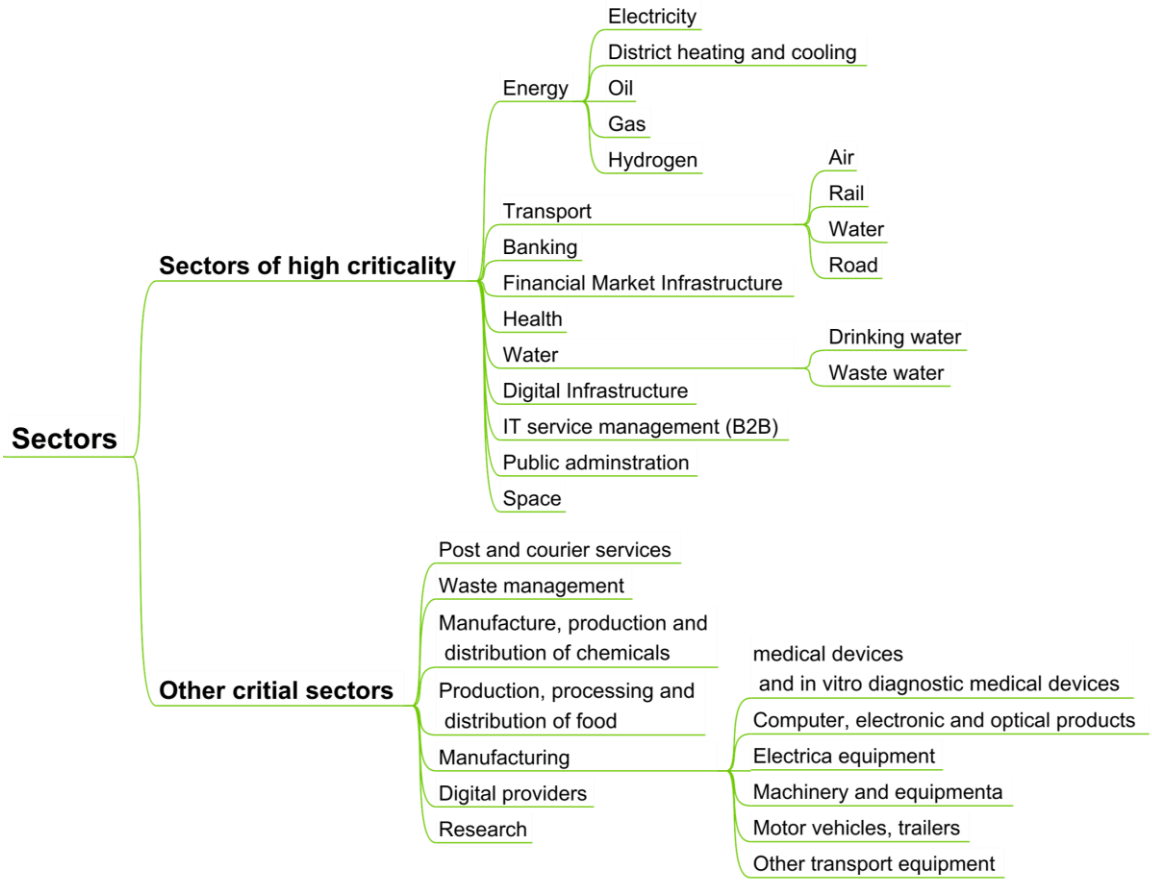

Figure 11: NIS2 sectors

Figure 11**Fehler! Verweisquelle konnte nicht gefunden werden.** shows the sectors of high criticality and other critical sectors It is important to note that the "Industry" sector also includes the chemical industry and automotive manufacturing.

Operators: Medium and large enterprises with 50 employees/10 million € turnover or more are affected, without system thresholds.

Cyber security: The requirements for operators and member states are increasing, cyber security must also be considered in supply chains. Operators in the EU must implement at least the following cyber security measures to protect the IT and networks of their critical services: Art. 21.

- Policies: Guidelines for risks and information security.
- Incident Management: Prevention, detection and management of cyber incidents.
- Business Continuity Management: BCM with backup management, crisis management.
- Supply chain: Security in the supply chain - through to secure development at suppliers.
- Purchasing: Security in the procurement of IT and network systems.
- Effectiveness: Guidelines for measuring cyber and risk measures.

- Training: Cyber Security Hygiene.
- Cryptography: Specifications for cryptography and encryption where possible.
- Personnel: Human Resources Security.
- Access control.
- Asset Management.
- Authentication: Use of multi-factor authentication and Single Sign on (SSO).
- Communication: Use of secure voice, video and text communication.
- Emergency communication: Use of secure emergency communication systems.

Cooperation: Supervision and cooperation in the EU between authorities and operators will be intensified, European jurisdiction sharpened.

Sanctions : Penalties and enforcement actions will be significantly extended - to maximum penalties of at least 7 or 10 million €, depending on the sector.

The EU member states must implement the minimum standard of NIS2 through national laws. Further information about this can be found in chapter 4.2.3.

4.1.4. Cyber Resilience Act

The Cyber Resilience Act (CRA) [CRA2024] was published on 20.11.2024 and came into force on 11.12.2024. It affects manufacturers of devices with digital elements that have a communication link (direct or indirect).

The date of application of the CRA is 36 months after the date of entry into force.
This means that

- From September 11, 2026, actively exploited vulnerabilities must be reported to national authorities and ENISA. See Article 14.
- From December 11, 2027, all requirements of the CRA apply. The CE mark will then document that a product with digital elements meets the requirements of the CRA.

Figure 12 summarizes the CRA timeline.

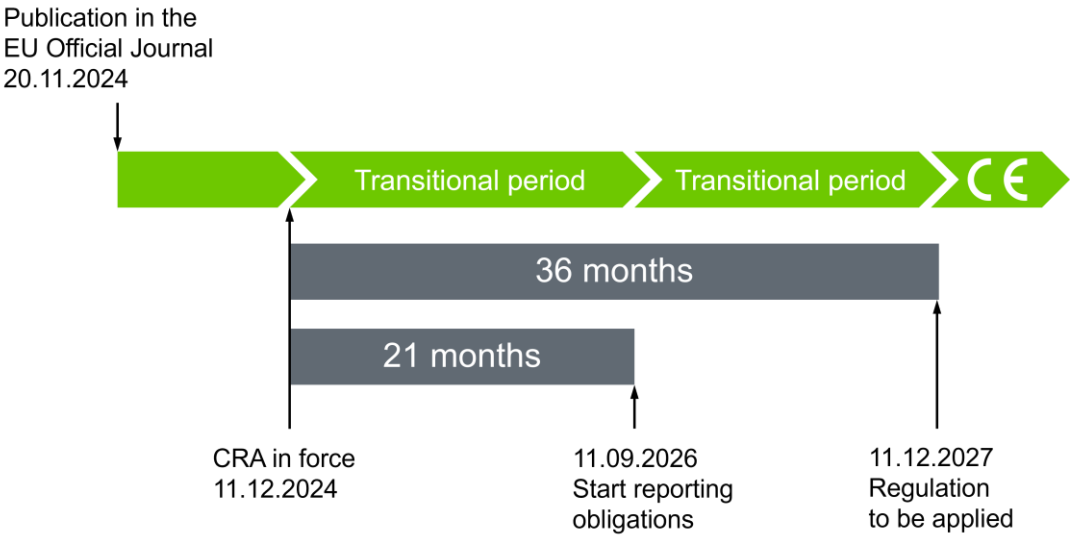

Figure 12: Timeline of the CRA

According to [KIR2022], the main aspects of the CRA concern the definition of cybersecurity regulations for placing hardware and software on the market in the EU. Obligations are defined for manufacturers, distributors and importers. These are essentially requirements for cybersecurity throughout the entire life cycle (at least 5 years). The harmonized standards to be followed are currently being drawn up. The aim of these standards is to enable a differentiated conformity assessment according to risk level. It can be assumed that the standards will essentially be based on the IEC 62443 series of standards.

Figure 13: Obligations of manufacturers according to CRA

Figure 13 shows the main obligations of manufacturers in accordance with the CRA. The CRA is relevant for operators and planners of production facilities insofar as manufacturers can be expected to comply with defined OT Security requirements from the 11.12.2027 deadline. This also supports the security along the supply chain required by the NIS2 directive.

4.1.5. Machinery Regulation

The EU Machinery Regulation [EUR2023] essentially deals with the aspects of functional safety. It is nevertheless mentioned here because it addresses protection against and the safety and reliability of control systems in sections 1.1.9 and 1.2.1 of Annex III. The Machinery Regulation is therefore also relevant with regard to OT Security .

The EU Machinery Regulation is in force. It does not need to be transposed into national law. There is currently a 42-month transition period; the regulation must be applied from 20.01.2027 at the latest. The Machinery Regulation replaces the previous Machinery Directive 2006/42 [EUR2006]. The book [HÜN2024] is recommended for further reading.

4.2. National German requirements

With the IT-Sicherheitsgesetz (engl. IT Security Act) [ITSichG2015], national German legislation has issued the first regulations on OT Security in critical infrastructures. European legislation now also requires the CER Directive (see chapter 4.1.1) and the NIS2 Directive (see chapter 4.1.3) to be transposed into national law. The following chapters provide a brief overview of national German legislation.

4.2.1. IT Security Act and BSI Criticality Ordinance

With the IT-Sicherheitsgesetz (engl. IT Security Act) [ITSichG2015] from 2015, the legislator defined requirements with regard to the IT security of critical infrastructures (KRITIS). The definition of critical infrastructures was regulated at the time by a separate legal ordinance [BSI-KritisV_2016]. In the edition at the time, the following infrastructures were covered by the ordinance: electricity supply, gas supply, fuel and heating oil supply, district heating supply, wastewater disposal, drinking water supply. The ordinance defined threshold values for the supply facilities. For example, sewage treatment plants with a population equivalent of 500,000 or more or power plants with a rated output of 420 MW or more are covered by the ordinance.

As part of the IT-Sicherheitsgesetz (engl. IT Security Act), a reporting office for incidents is set up at the Federal Office for Information Security (BSI) and a reporting obligation for critical incidents is defined.

The law also stipulates that

> *"Operators of critical infrastructures are obliged to take appropriate organizational and technical precautions to prevent disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes that are relevant to the functionality of the critical infrastructures they operate no later than two years after the legal ordinance pursuant to Section 10 (1) comes into force."* [ITSichG2015]

The operators of critical infrastructures were also obliged to set up a contact point and had to demonstrate compliance with the requirements. In addition, the [ITSichG2015] summarizes a number of other amendments to other laws that relate to the topic of critical infrastructures and IT security.

In 2021, the IT-Sicherheitsgesetz 2.0 [IT_SIG_2.0] was published, which updated the law from 2015. The group of affected companies was expanded and municipal waste disposal was included as critical infrastructure. Systems for attack detection became mandatory. The associated ordinance has since been replaced by the “Dritte Verordnung zur Änderung der BSI-Kritisverordnung” (engl. "Third Ordinance Amending the BSI Critical Infrastructure Ordinance") [BUN2023]. Here, for example, terminals for liquid gas were also defined as critical infrastructure.

In view of the expected implementation laws for the CER and NIS2 directives, it is to be expected that the IT Security Act will also have to be adapted so that the three laws do not result in contradictions or multiple regulations.

4.2.2. KRITIS umbrella law

Act implementing Directive (EU) 2022/2557 and strengthening the resilience of critical installations" [BMI2024] the so-called KRITIS Dachgesetz (eng. Umbrella Act for Critical Infrastructure Protection) was described in chapter 4.1.1.

4.2.3. NIS2 Implementation Act

The NIS 2 Implementation and Cybersecurity Strengthening Act [NIS2UmsuCG] was passed by the Federal Cabinet at the end of 2024 and was subsequently due to be passed by the Bundestag. Due to the government reshuffle at the end of 2024, the legislative project could not be finalized. An updated draft bill with a slightly different name had been in the process of being voted on by associations since June 23, 2025. On 11.09.2025, the German Bundestag debated the NIS2 Implementation Act [NIS2_DE_2025] in the version dated 08.09.2025 at first reading.

5. Measures for the implementation of OT Security in production

Chapter 3 provided an overview of the norms and standards relevant to OT Security , followed by a summary of the legal framework in chapter 4. Operators and planners of production facilities are now faced with the task of deriving an appropriate procedure from this. However, the problem for SMEs is that these standards and laws are very extensive and in some cases still incomplete. It is therefore often difficult for employees in SMEs to make an assessment in relation to their own company.

A sensible approach is therefore to first take stock to be able to describe the current situation. An initial assessment can be provided by a quick check (e.g. www.vds-quick-check.de), which provides an initial classification of the company in terms of IT security. One check each for the office and production areas is available on this website. Comparable checks for OT inventory are also available from ISACA [ENN2021] or the tool SiToM [MIT2025b] from Mittelstand Digital.

To provide SMEs with an easy introduction to IT security in the production area, a ten-step plan for establishing IT security in the production area is proposed below as an initial measure. These ten points are:

1. Management commitment
2. Organization of responsibilities and processes
3. Creation of a guideline
4. Personnel
5. Procurement and provision of knowledge
6. Identification, evaluation and protection of assets
7. Regulation of external access to production facilities
8. Data backup
9. Handling malfunctions and failures
10. Recognizing IT security incidents

The following chapters will deal with these ten points and describe the necessary measures for establishing an IT security process in the production area. The literature usually focuses heavily on points 6 and 7, but it should be noted that IT security should be viewed as a holistic process that includes all points.

5.1. Management commitment

IT security must be established as a top-down process within the company. It can only be implemented in the company if there is a corresponding commitment from management. To this end, management should draw up an IT security strategy for the company (or have one drawn up) that covers the office and production areas. The strategy should define clear objectives and corresponding responsibilities.

The following points are recommended as a first step in this process:

- Establish a top-down process to establish OT Security in the company.
- Utilization of synergies between IT and OT Security
- Creation of an OT Security strategy.
  - Definition of objectives.
  - Definition of responsibilities.
- Initiation of a project for processing the tasks.
- Definition of responsibilities.
- Provision of resources:
  - Internal.
  - External if necessary.
  - Personnel and financial

It is recommended to define a project for the initiation of the process and to provide it with the necessary internal and, if necessary, external resources. The procedure described here is comparable to the introduction of a quality management process.

5.2. Organization of responsibilities and processes

Once the project has started, management must define the relevant responsibilities. As OT Security is to be seen as an overarching process, overall responsibility should be defined in the form of a Chief Information Security Officer (CISO), who is responsible for IT and OT Security. It must be ensured that the person has the necessary knowledge in the office and production areas. If necessary, the IT security officer can delegate tasks. The IT security officer should form the information security team together with other employees and a management representative. This team is responsible for implementing the IT security strategy and for dealing with disruptions, failures and IT security incidents.

The basis for the organization of IT and OT Security is what is known as an information security management system (ISMS). The BSI writes about this in the basic protection module IND.1: Process control and automation technology in Part A1 and following [BSI2021b]:

- "An information security management system (ISMS) for the operation of the OT infrastructure SHALL exist either as a stand-alone ISMS or as part of an overall ISMS and SHALL explicitly include within its scope the definition of objectives and values, processes, roles, responsibilities and requirements for OT.
- The management level of the institution SHALL initiate, manage and control the security process. The institution SHALL establish a security organization that regulates the roles and responsibilities for the information security of the OT infrastructure and components.
- An overall responsible person for information security in the OT area SHALL be appointed and made known within the institution.
- There SHALL be a process for writing, communicating, implementing, updating, evaluating and improving tangible specifications (guidelines) for specific subject areas in the process area."

Appropriate personnel must be assigned to the topic/project to ensure continuous work. The reporting channels must be defined. The delegation of tasks and the involvement of top management must also be regulated. Both the NIS2 guideline [NIS2_en] and [ISO_IEC_27001] define the responsibility of top management with regard to IT and OT Security . It should be noted that suppliers and system integrators must also be included in the processes.

5.3. Creation of guidelines

The topic of OT Security must be described by the company in one or more corresponding guidelines that provide staff with basic rules of conduct. Staff can only behave accordingly if they know what is expected of them in terms of IT security. Examples of topics for the guideline(s) could be

- Basic rules of conduct in the production area:
  - Private use.
  - Introduction of software updates into the production system.
  - Prior checking of software updates.
- Dealing with safety devices.
- Disclosure of login information.
- Information flow in case of absence.
- Abuse control.
- Regulations for suppliers/integrators

The guideline should also make it clear that misuse is to be monitored and that sanctions are to be expected in the event of misconduct. Appropriate coordination with the works council is generally required.

5.4. Personnel

Personnel are a decisive factor for OT Security . Adequate know-how and staff training can make a decisive contribution to OT Security in the company.

The BSI writes in the “Grundschutzmodul” (engl. basic protection module) IND.1 in part A2 sensitization and training of personnel [BSI2021b]:

- "Operational staff SHALL be regularly informed and sensitized to relevant IT security threats in the OT area. OT managers SHALL be regularly informed or trained on the threat situation and the need for action."

At this point, reference should also be made to the training obligation for management in accordance with the NIS2 Directive [ATU2025].

A confidentiality agreement must be signed by the employee upon joining the company. During the induction phase, new employees must be instructed in the OT Security guidelines and any other guidelines.

Appropriate measures must be taken when employees leave the company. VPN access for these employees must be blocked and passwords changed. This also applies to shift accesses .

5.5. Procurement and provision of knowledge

A survey on the evaluation of security advisories in the production environment by KMI [WUL2022] showed that only 50% of the companies surveyed monitor and evaluate security advisories from automation technology manufacturers. For this reason, a process must be established within the company to ensure that the company obtains the relevant, up-to-date information. Possible sources for obtaining information on vulnerabilities could be

- Information from the manufacturers of automation systems. For example:
  - z. B. ABB [ABB2025]]
  - z. e.g. Siemens [SIE2025]
  - z. e.g. Wago via CERT@VDE :[WAG2025]

- Consolidated information on vulnerabilities (IT and OT):
  - Information from ICS-CERT (Homeland Security of the U.S.A.) regarding known vulnerabilities of automation systems [DHS2025]
  - CVE Common Vulnerabilities and Exposures [MIT2025a]
  - European Union Vulnerability Database [ENI2025]

Ensure that knowledge is up to date. In some cases, it is possible to subscribe to alerts (messages about vulnerabilities detected by the manufacturer) for certain systems via an E-mail distribution list. People must be appointed in the company to evaluate these alerts and derive measures for the company from them.

The monitoring and evaluation of vulnerability reports is time-consuming. The German Federal Office for Information Security (BSI) has therefore been promoting the provision of vulnerability reports in machine-readable form via the Common Security Advisory Framework (CSAF) [BSI2025b] for some time. In conjunction with an asset database of the operator, this would enable automated evaluation and assignment of vulnerability reports.

In addition to specific knowledge in relation to known vulnerabilities, the general knowledge of employees must be established and kept up to date through awareness-raising, training and further education.

5.6. Identification, assessment and protection of assets

This section describes how the assets of a production plant are systematically recorded, assessed about their risk and protected if necessary. This is done in accordance with the VDI 2182 series of standards. The IEC 62443 series of standards provides a comparable procedure. The steps shown in Figure 10 are used to analyze the automation system. Chapter 3.2.2 describes the "Plan-Do-Check-Act cycle" (PDCA) and the necessary steps.

The result of this analysis is:

- List of all assets.
- List of threats affecting the assets in the form of a threat matrix.
- List of all relevant protection goals in the form of a threat matrix with relevant protection goals.
- List of assessed risks affecting the assets.
    - The VDI 2182 series of standards makes suggestions for the structure of such lists.
- List of possible protective measures and evaluation of their effectiveness and costs.
- List of selected protective measures to be implemented.
- Report on the implementation of protective measures.
- Results of the process audit to assess the effectiveness of the selected measures.

Typical protective measures that are the result of the described process usually result in a so-called Defense in Depth concept [DHS2016], [KUI2006]. The following figures show examples of selected elements of a defense in depth concept.

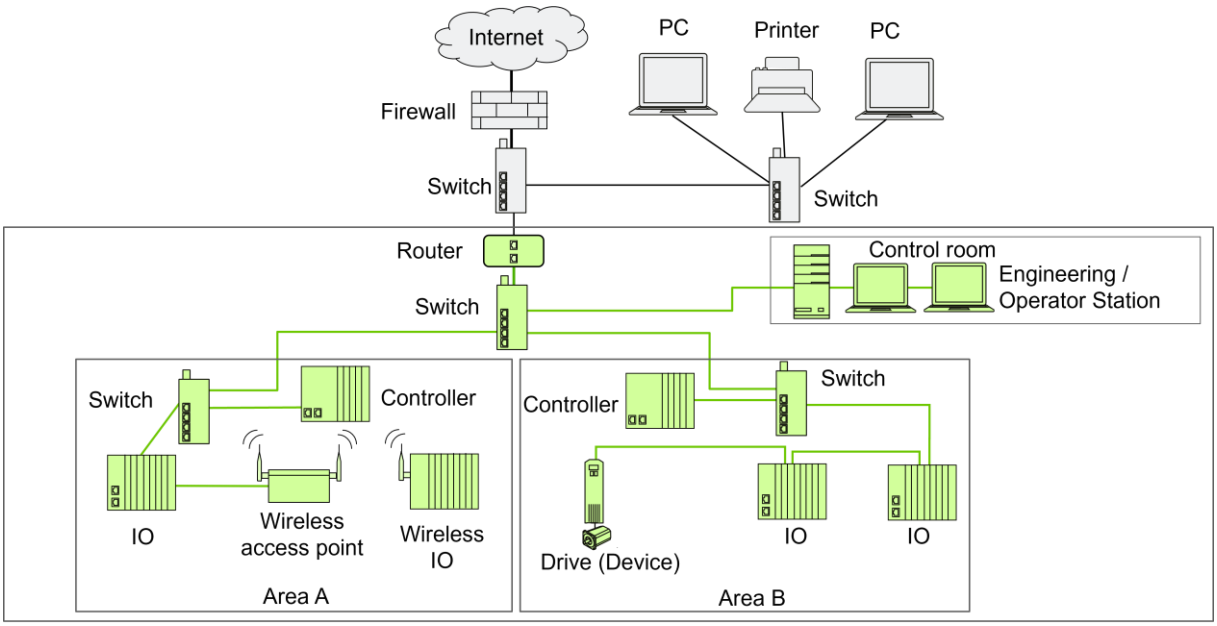

Figure 14: Example system with office and production area

Figure 14 shows a production plant consisting of the two plant areas A and B. The control room area is located above the production plant. The office area is shown above it. It is assumed that the company is separated from the Internet by a firewall . A connection to the Internet is required, for example, to obtain software updates or to store data in the cloud.

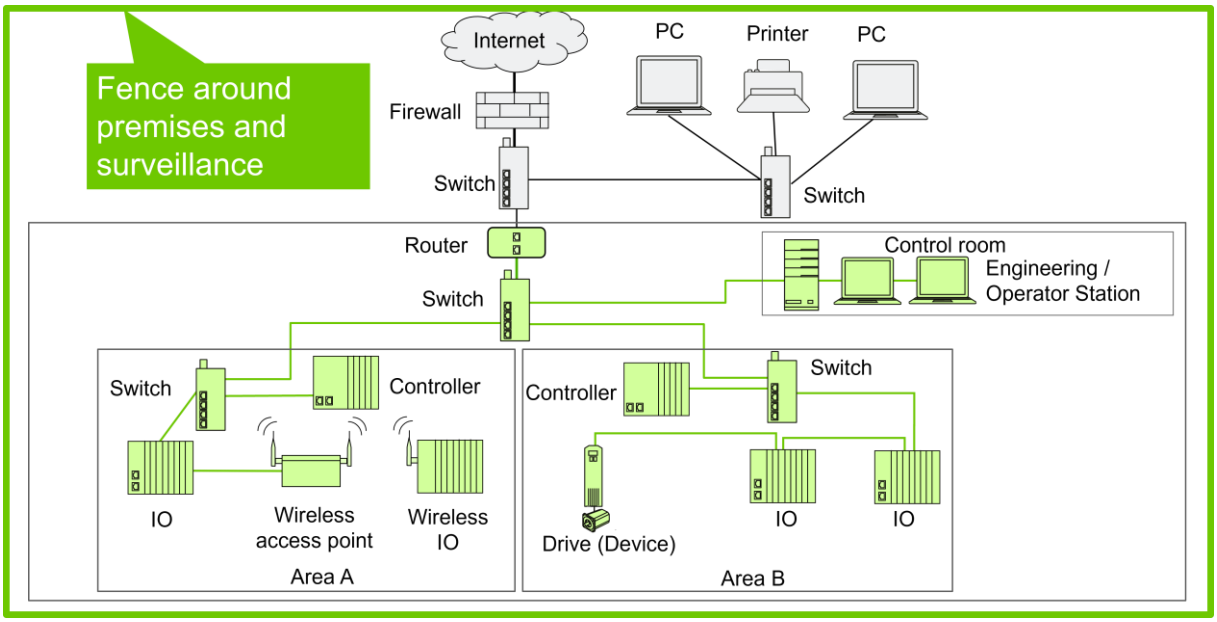

Figure 15: Perimeter protection

As a first measure, as shown in Figure 15, the entire property can be protected against intrusion from outside, e.g. by a fence. This measure prevents unauthorized people from gaining access to the site and represents the first barrier for attackers. It should be noted that monitoring the fence, e.g. by means of AI-supported video surveillance as described in [SEC2024], makes sense. Perimeter protection is also part of the CER Directive [CER_en]. Companies covered by this directive should therefore take the CER directive into account when selecting perimeter protection.

An incident has been known since 2008 in which a cyber attacker was able to overcome a double fence and shut down a power plant through a cyber-attack [PAN2008]. This means that the fence can only be one of several protective measures. A fence is not an obstacle for radio waves. If wireless communication is used in the production plant, a corresponding risk assessment is required. This applies, if the radio link is close to the fence.

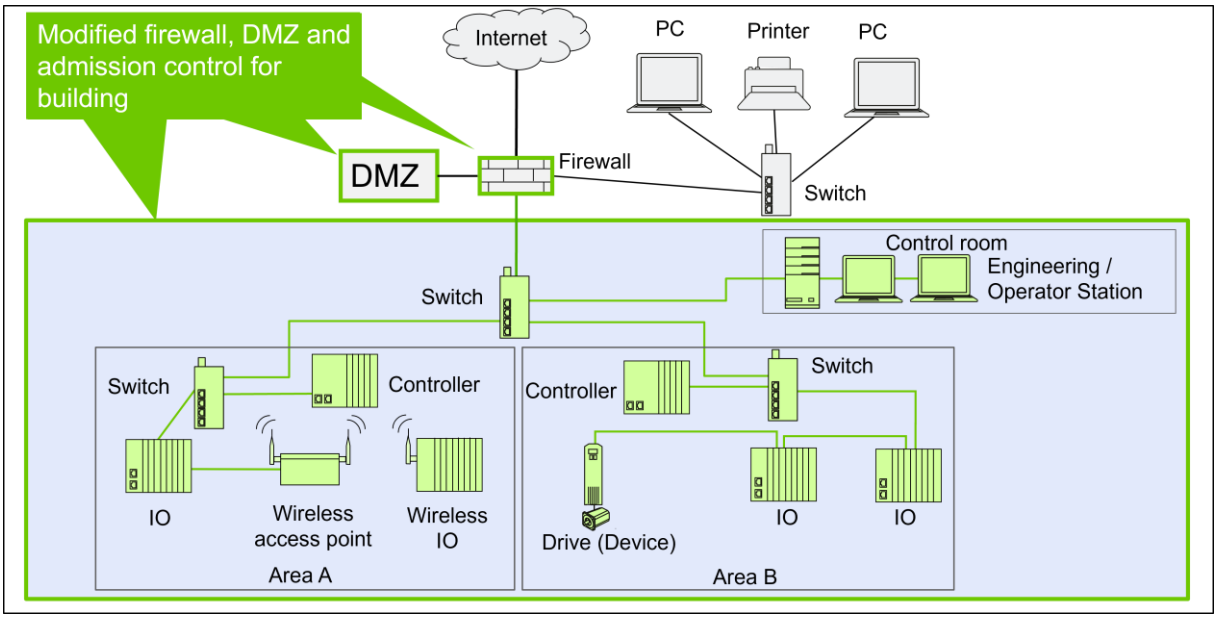

Figure 16: Modified firewall, DMZ and building access monitoring

Figure 16 shows a modified configuration of the firewall as the next protective measure. This is now configured in such a way that access to the automation system (blue background color) from outside the company is not permitted. At the same time, connections to the office area necessary for the operation of the system are permitted. This separation is specified in [IEC_62443-3-3] under the keyword "Protection of the zone boundary ". The function of the router can also be taken over by the firewall. The router is therefore not required.

A demilitarized zone (DMZ) can also be connected to the firewall at this point. This serves to separate the IT and OT networks. They form an isolated network zone between the "insecure" external network - such as the Internet or the corporate network and the production network, which is particularly worthy of protection. Services such as remote access , data storage or update servers , which need to communicate with both the outside world and the production environment, are typically operated in this intermediate zone. This separation prevents a successful attack on publicly accessible systems from gaining direct access to the production systems. The DMZ acts as a buffer.

As a further measure, an access control system is installed for the building in which the production facility is located in accordance with**Fehler! Verweisquelle konnte nicht gefunden werden.**Figure 16. These measures separate the production area from the office area and from the Internet in terms of data. In addition to the fence around the factory premises, a second, tighter access protection has been implemented.

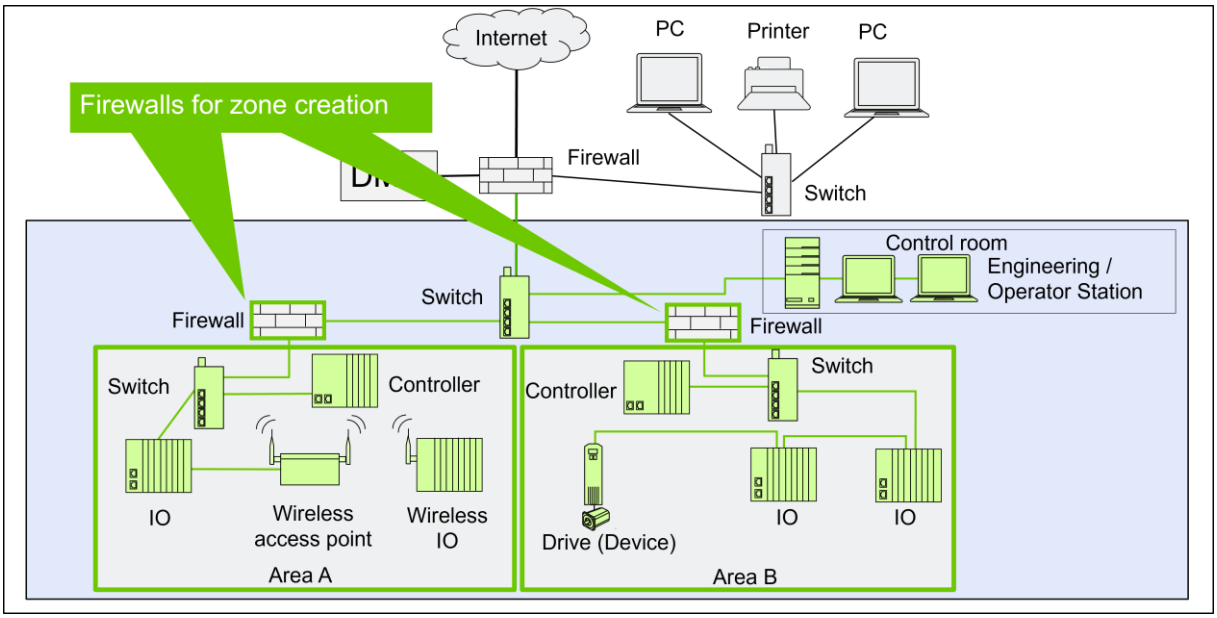

Figure 17: Division of the production area into zones

Figure 17 shows a further subdivision of the production plant. The production plant is divided into two sub-areas (gray background). Each of these areas is in turn separated from the control room area by a firewall. In addition, the components in the sub-areas could be further protected, e.g. by installing them in a locked control cabinet.

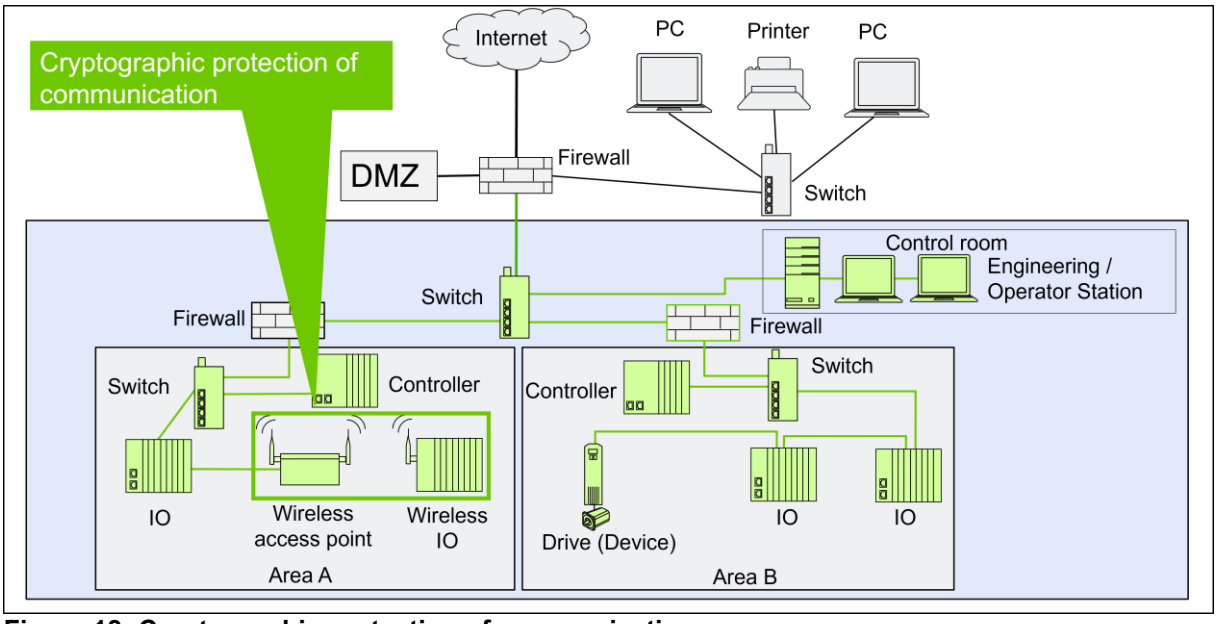

Figure 18: Cryptographic protection of communication

Figure 18 shows the protective measure for a wireless access point using encryption. Even if standard WLAN access points on the market offer encryption as standard, care must be taken to select a sufficiently secure method and sufficiently strong passwords.

In addition to the standard protection of WLAN communication, it will also be possible in future to secure wired communication cryptographically. PROFIBUS & PROFINET International (PI) have developed a security concept for the PROFINET communication protocol that protects integrity and authenticity and, if required, the confidentiality

of PROFINET communication. For more information on PROFINET, see [NIE2023a], [PNO2019], [WAL2023].

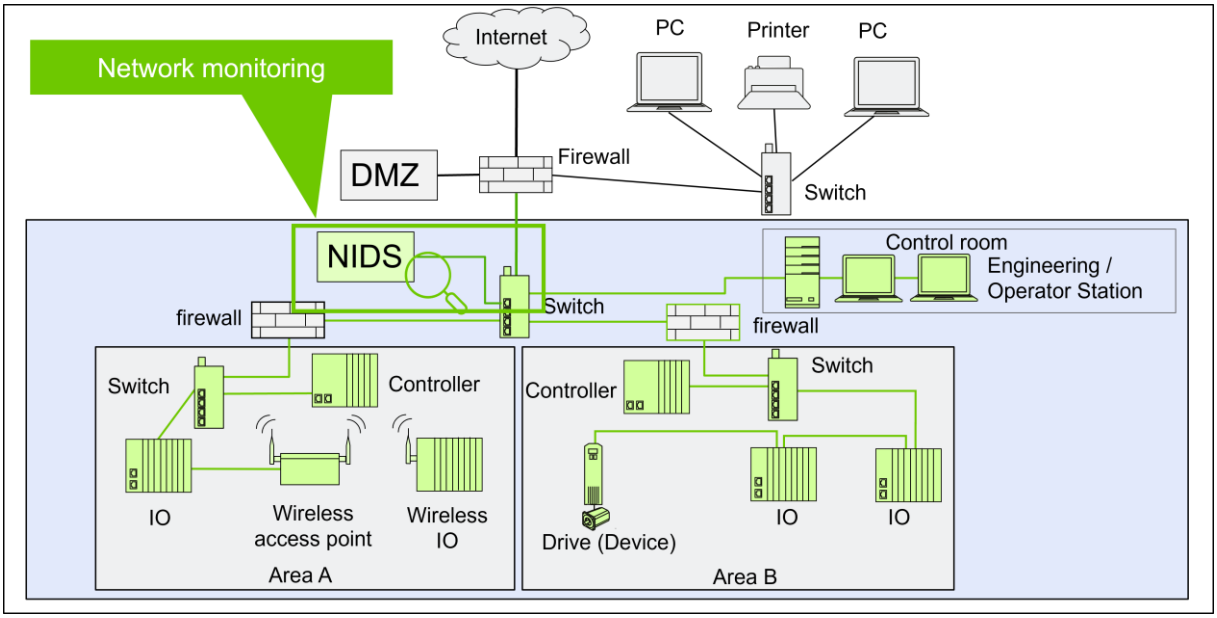

Figure 19: Network monitoring

Figure 19 shows monitoring as the last measure, e.g. via a network monitoring system. A network monitoring system (Network Intrusion Detection System-NIDS or Intrusion Detection System-IDS) monitors network traffic for anomalies at certain points. Continuous monitoring of the automation system is included in requirement SR6.2 of [IEC_62443-3-3]. A NIDS is one of several possibilities.

The measures presented here are just a few examples. There are other measures that will not be discussed here for reasons of space. Examples of these include

- Virus protection/anti-malware / endpoint protection.
- Application whitelisting.
- Access restriction for transportable media.
- Authentication of staff and network users.
- Limiting access to the network by switching off unused network ports (hardening).

Although this part of the ten-point program is the most complex, the other points should not be neglected.

5.7. Regulation of external access to production facilities

External access to production facilities for remote diagnostics and remote maintenance purposes is a particularly critical process from the perspective of OT Security . For this reason, this topic is described in a separate section.

Known incidents can be traced back to the use of remote access [TOF2009], [SAN2016], [PIT2023]. Further attacks via remote access are documented in [CLA2024b]. For this reason, special security measures apply to these accesses. The BSI basic protection module IND.3.2 Remote maintenance in an industrial environment [BSI2022a] can provide good guidance. Here, the BSI describes the basic procedures for setting up remote access. The main requirements of the BSI are:

- Establish a standardized solution. This standardizes the hardware and processes used and thus reduces the administrative effort.
- Arrangement of the remote maintenance components in a separate zone (DMZ)
- Do not allow full access to an entire (sub)network but only to dedicated endpoints.
- Establish the remote maintenance connection from within the company to the outside.
- Use dedicated systems that are only used for this purpose.
- Only established protocols such as IPsec, SSH or SSL/TLS in current versions are used to establish a tunnel between two endpoints or networks.
- The connection between the company and the diagnostic site must be encrypted. Sufficiently strong cryptographic procedures are used for encryption.
- Only one user per account should be provided. Group accounts should be avoided.
- Multi-factor authentication procedures shall be used.
- If passwords are used, corresponding password specifications must be created and observed.
- Mechanisms for detecting attacks on password-based authentication procedures must be used.
- Create a risk analysis.
- Observe the minimization principle (as few connections as possible).
- Establish processes for releasing and blocking remote access.
- Provide guidelines for the personnel who carry out remote maintenance. E.g. prohibition of remote maintenance via cell phones.
- Restrict the remote access to a defined time window. Automatic disconnection after a certain period of time should be implemented.
- Use of log functions, analysis of log information.

The referenced document contains further information. Only the essential points are reproduced in this document.

In a study, the company Claroty investigated how many different remote access solutions are operated in simultaneously production plants. [CLA2024a].

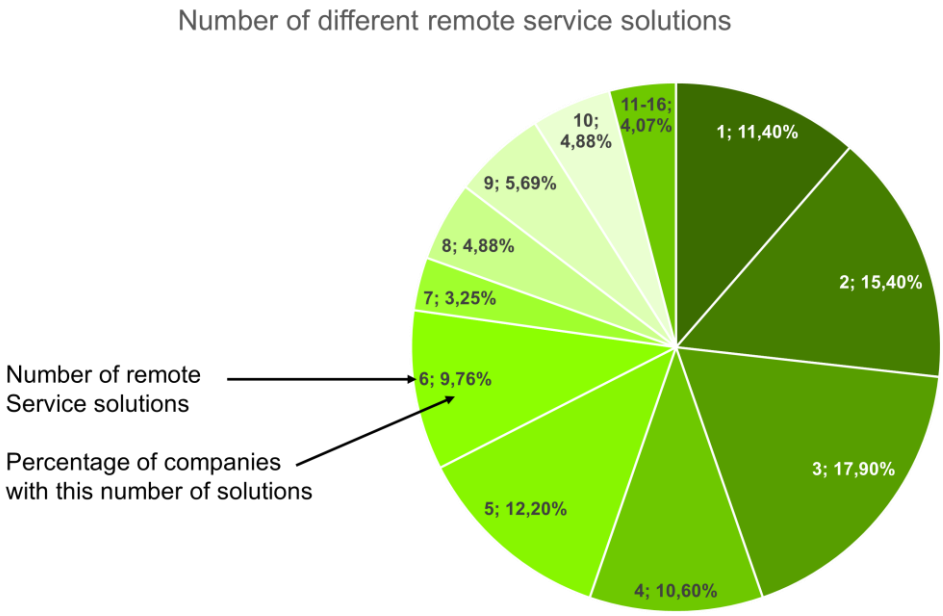

Figure 20: Number of remote maintenance solutions in a company (derived from [CLA2024a])

Figure 20 shows the number of different remote maintenance solutions used by the companies surveyed. The authors of the study say:

> *"Almost 22% have eight or more, and some manage as many as 15 or 16 remote access tools."*

From this it can be concluded that timely standardization on one or a few remote access tools significantly reduces maintenance effort and risk.

Further information on remote maintenance can be found, for example, in the NAMUR recommendation "Remote access - IT security requirements for remote access" [NE_135_en]. A summary of many guidelines on remote maintenance and an overview of the various technical approaches can be found in [LAN2022].

5.8. Data backup

The attack on the Ukrainian energy supply network in 2015 is described in [ZET2016] and [SAN2016]. Among other things, the hard disks of control systems were rendered unusable in this attack with the help of the "KillDisk" software. Triggering a total loss of data is a well-known method of attack. Ransomware attacks on production facilities are also known. In 2020, for example, a pipeline on the east coast of the USA was rendered inoperable by ransomware [CYB2020]. The aim of a ransomware attack is to encrypt data and demand a ransom to restore the data. For this reason, data backup is particularly important in the production sector.

A concept must therefore be developed for the control of catastrophic data loss (deletion of all data including the operating system) for the OT area. Part of a data backup

concept is the regular and complete backup of all data of the automation system. The recovery routines must be documented and tested.

In view of the continuing spread of encryption trojans/ransomware, the backup systems and the backup concept should take this threat into account. In its ransomware catalog of measures [BSI2022c], the BSI formulates the following general requirements, which can also be applied to the OT sector:

- "A backup is the most important protective measure to ensure the availability of data in the event of a ransomware incident. Every institution should have a data backup concept (IT baseline protection: B 1.4 Data backup concept) and implement it.
- At least one copy should therefore be backed up offline. These copies are separated from the institution's other systems after the backup and are therefore protected against remote attacks.
- Offline backups can be made with separate tapes, in a separate archive with the necessary physical access or in a cloud storage facility that is completely separate from your own network.
- A backup always includes the planning and preparation for restarting and restoring the data."

The Mittelstand Digitalzentrum Hannover has developed a best practice guide on encryption Trojan-resistant data backups in the OT sector [PUL2024b]. People who are responsible for backups in the OT sector can use the following key questions as a guide:

- Is the backup concept documented and known to employees?
- Is there a backup plan (3-2-1 strategy)?
    - Are **3** copies available (one of which is the original + 2 backups)?
    - **2** different media (internal hard disk /external hard disk).
    - **1** storage location.
- Is compliance with the backup plan monitored and/or the execution of the backups documented?
- Is the backup physically secured (fire / water / theft)?
- Is the backup an offline backup or otherwise protected against Trojans?
- Has the restore of backups been tested?
- Can the backup be restored to replacement hardware in the event of a hardware failure?
- Is there an emergency plan for restoring systems from the backup?

Further specifications on the subject of backups can also be found in [ISO_IEC_27002] under the keyword "Data backups".

5.9. Handling faults and outages

Fast and efficient handling of faults and outages is necessary to be able to resume operations quickly after such an incident. To this end, it is essential that the term is clearly defined. The reporting type and reporting channels must be defined and documented. It must be determined which type of incident falls into this category. Furthermore, a plan for external communication must be drawn up. The reactions to faults and outages must be defined and procedure models (restart plans) for dealing with such incidents are required.

If an incident occurs, the first priority is to restore normal operation. This is followed by an investigation into the cause, documentation of the damage and follow-up work to prevent future incidents.

The BSI Standard 100-4 Emergency Management [BSI100-4] provides a good basis for sketching an emergency plan. The "BSI Security Incident Response Guide" [BSI2022d] summarizes the necessary steps in the event of an emergency as follows:

- Reporting obligations.
- Digital rescue chain.
- Involvement of specialist personnel.
- Standard procedure.
- Attack scenarios and countermeasures.
- Forensic procedure.
- Data collection.
- Data analysis.
- Remote support.
- Emergency operation.
- Follow-up.

5.10. OT Security - Detecting incidents

The incidents described in the chapter 5.9 can initially be of a general nature. IT security incidents form a sub-category of these incidents that require special handling. In principle, the procedure described in chapter 5.9 applies to IT security incidents. In addition, preventive measures are useful for detecting and averting IT security incidents. A survey conducted by the SANS Institute [SAN2015] revealed that 15 % of the companies surveyed stated that it had taken more than a month to detect an incident. The Ponemon Institute [PON2017] cites a duration of 170 days between an infestation and the detection of a security incident.

For this reason, the recording, storage and evaluation of security-relevant events (security logging) is a key success factor for the early detection of cyber incidents. As a rule, the events from the OT area are forwarded to a higher-level security information and event management system (SIEM). A SIEM is used to centrally record, analyze and correlate security-relevant data within an IT and OT infrastructure. It continuously

collects events from various sources such as control components, firewalls, servers, end devices and cloud services and evaluates them in real time to detect potential threats at an early stage. By intelligently linking seemingly isolated incidents, a SIEM can identify patterns that indicate attacks or security breaches.

The topic of security logging can be explored in more depth using the following sources:

- Monitoring and Anomaly Detection in Production Networks [BSI2019].
- BSI baseline protection: OPS.1.1.5: Logging [BSI2021a].
- BSI basic protection catalog - DER.1 Detection of security-relevant events [BSI2021a].
- Minimum standard of the BSI for logging and detection of cyber-attacks according to § 8 Section 1 sentence 1 BSIG [BSI2023b].
- Logging and log management - The authoritative guide to understanding the concepts surrounding logging and log management [CHU2013].

6. Outlook

The 10-step action plan presented in chapter 5 offers an initial approach to implementing OT Security in the production area for SMEs . Although it is suitable for providing adequate protection for a production facility, there are still some challenges that need to be addressed in the future.

Previous concepts focus heavily on defense from the "outside". [BER2023] shows that employees acting intentionally and unintentionally cause a significant proportion of cyber-attacks. See Figure 21. Therefore, outward-facing protection is no longer sufficient.

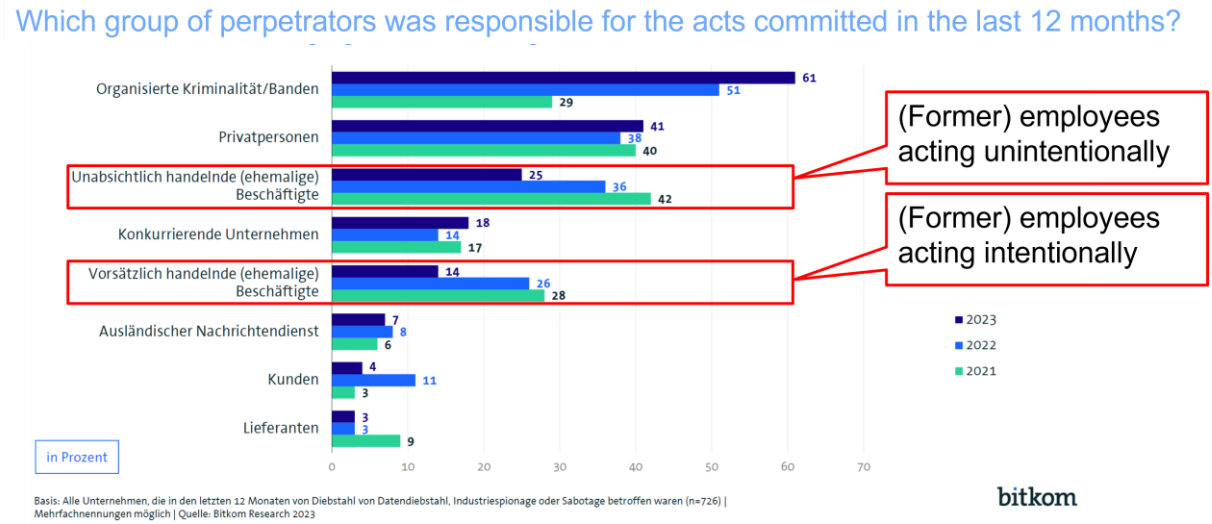

Figure 21: Proportion of internal perpetrators [BER2023]

Future concepts must therefore focus more strongly than before on protection against internal perpetrators. This includes, for example, the installation of automation components in locked control cabinets, network access monitoring and the introduction of user accounts for automation systems.

Increasing horizontal and vertical integration in the context of Industry 4.0 will mean that traditional protection mechanisms will only be effective to a limited extent. The number of network nodes will increase, and the effort required to ensure OT Security will rise. IT/OT convergence must be given larger consideration when it comes to security. The convergence of IT and OT presents companies with the challenge of securely linking two worlds that were previously only loosely coupled. The closer coupling of IT and OT creates new areas for attacks. OT components that were previously operated in isolation suddenly become easier to access through networking. For more in-depth information, here is a research paper [AMI2024] and a field report [GAN2023].

NAMUR described the requirements for future automation systems in [NE_153_en] back in 2015. The basic idea is the "Secure by Design" approach. Instead of isolating the devices, security functions will be integrated into the devices in future, which will allow secure communication even under real-time conditions. The procedure for

developing automation components using this approach is described using the example of an Ethernet APL transmitter in [NIE2023b]. Further considerations on the topic of "Secure by Design" can be found in [FLU2022].

Another major challenge is certainly the timely fulfillment of legislative requirements. The NIS2 Directive and Cyber Resilience Act (CRA) will keep operators, planners and manufacturers very busy in the near future.

For the implementation of OT Security , however, the usual measures should be implemented and in particular the "low hanging fruits", the goals that can be achieved with limited effort, should be harvested. Here, a great gain in security can be achieved with little effort.

7. List of figures

Figure 1: Cyber incidents from the building automation sector [LI2023] 9
Figure 2: Horizontal and vertical integration 10
Figure 3: ISO 27001 / ISO 27002 and IEC 62443 as components of a cybersecurity strategy (based on [NIE2024b]) 13
Figure 4: Overview of norms and standards for OT Security 14
Figure 5: Number of valid ISO 27001 certificates in Germany in the years 2006 to 2023 [STA2025a] 15
Figure 6: Prioritization protection goals for the office area (IT) and automation technology (OT) 16
Figure 7: Parts of IEC 62443 17
Figure 8: Risk analysis derived from [IEC_62443-3-2] 18
Figure 9: Responsibilities and associated standard parts in the security process 20
Figure 10: Process model according to [VDI_2182_1_en] 21
Figure 11: NIS2 sectors 29
Figure 12: Timeline of the CRA 31
Figure 13: Obligations of manufacturers according to CRA 31
Figure 14: Example system with office and production area 38
Figure 15: Perimeter protection 39
Figure 16: Modified firewall, DMZ and building access monitoring 40
Figure 17: Division of the production area into zones 41
Figure 18: Cryptographic protection of communication 41
Figure 19: Network monitoring 42
Figure 20: Number of remote maintenance solutions in a company (derived from [CLA2024a]) 44
Figure 21: Proportion of internal perpetrators [BER2023] 48

8. List of tables

Table 1: Top 10 threats [BSI2022b] extended by fields of action 11
Table 2: Meaning of the abbreviation STRIDE 22

9. Index

Access control ... 25, 30, 40
Access restriction ... 42
Anomaly Detection ... 47
Anti malware ... 42
Asset ... 20
Asset Management ... 30
Asset owner ... 20
Attack detection ... 33
Authentication ... 19, 30, 42
Availability ... 19
Backup ... 44, 45
Basic protection catalog ... 14
BSI ... 14, 23
BSI basline protecton ... 23
building automation ... 9
Building automation ... 8, 9
Business Continuity ... 29
CER directive ... 27
CERT@VDE ... 37
CIP-Security ... 24
Cloud ... 39
CMMS ... 10
Colonial Pipeline ... 8
Conduits ... 18
Confidentiality ... 19
Contact point ... 32
CRA ... 30
Cryptography ... 30
CSAF ... 37
CSET ... 22
CVE ... 37
Cyber attack ... 7
Cyber resilience act ... 30
Cyber-Resilience-Act (CRA) ... 27
data sovereignty ... 10
Demilitarized zone ... 40
Denial of Service ... 12
DMZ ... 40
Emergency communication ... 30
Emergency management ... 46
EtherNet/IP ... 14, 24
EU machinery regulation ... 31
Evaluation methodology ... 19
Event-Logging ... 24
Events ... 19
Faults ... 46
Federal Office for Information Security ... 23
Firewall ... 39
Foundational Requirements ... 19
Grundschutz ... 36
Guidelines ... 14, 36
Hardening ... 42
Horizontal integration ... 9
IACS ... 24
ICS ... 23
ICS security ... 23
ICS security compendium ... 23
ICS-CERT ... 14
ICS-Security ... 6
IEC 60870-5-101 ... 7
IEC 60870-5-104 ... 7
IEC 61850 ... 7
IEC 62351 ... 14
IEC 62443 ... 16
Incident ... 46
Incident Management ... 29
Industroyer ... 7
Information Security Management System ... 12
Integrator ... 22
Internal perpetrator ... 25
International Maritime Organization IMO ... 24
Internet ... 39
Intrusion Detection System-IDS ... 42
ISMS ... 12, 14, 15, 35
ISO 27000 ... 15
ISO 27001 ... 13
ISO 27002 ... 13
IT baseline protection compendium ... 15
IT security incidents ... 7
IT-Security ... 6
IT-Sicherheitsgesetz ... 32
IT-Sicherheitsgesetz 2.0 ... 33
Knowledge ... 37
KRITIS ... 32
KRITIS-Dachgesetz ... 33
Logging ... 18, 19, 24, 46, 47
Machinery regulation ... 31
Management Commitment ... 34
Manufacturer ... 20, 22
Maritime sector ... 9, 24
Microsoft Threat Modelling Tool ... 22
Minimization priciple ... 43

MQTT 10
NAMUR 14, 25
Network Intrusion Detection System - NIDS 42
NIS directive 28
NIS2 directive 27, 28
NIS2-Umsetzungsgesetz 33
NIST SP 800-82 14
Norms 14
ODVA 14, 24
Office area 40
OPC 7
OPC-UA 10
Operational Technology 6
Operator 17
Operator 20
Operator 23
Originator 21
OT 6
OT Security 1, 3, 6, 7, 9, 10, 11, 12, 14, 16, 17, 18, 19, 20, 22, 23, 24, 25, 27, 31, 32, 34, 35, 36, 37, 42, 46, 48, 49
Outages 46
Passwords 41
PDCA 21, 25
Personnel 30, 36
Petya/NotPetya 7
Phishing 11
Plan-Do-Check-Act 21
Planner 20
PROFINET 14, 16, 19, 24, 41
Protection Zone Boundary 40
Quick-Check 34
Ransomware 7
Remote access 40
Remote diagnostics 42
Remote maintenance 24, 25, 43, 44
Remote service 8, 23
Requirements 19
Responsibilities 35
Restart plan 46
Restricted data flow 19
Risk 20
Risk analysis 18
Risk reduction 20
Sanctions 30
Sectors 28
Security level 18
Security lifecycle 17
Service providers 17
SiToM 34
SME 3, 6, 12, 16, 23, 34, 48
Social engineering 11
SolarWinds 8
Standards 14
STRIDE 22
Sunburst 8
supply chain 8
Supply chain 10, 29
Supply chain security 8
Supply chain security 8
System integrator 20
System integrity 19
Threat 20
Top 10 threats 10, 23
Training 30
Update server 40
Use control 19
User 20
VDI/VDE 2182 ..... 14, 20
VdS 16
VdS 10000 14
VdS 10020 ..... 14, 23
vertical integration 10
Vertical integration 9
Virus protection 42
Vulnerability 21
WannaCry 7
Whitelisting 42
Zones 18

10. Bibliography

[ABB2025] ABB Asea Brown Boveri Ltd: Cyber security alerts and notifications. URL: http://new.abb.com/about/technology/cyber-security/alerts-and-notifications, 29.11.2016.

[ABS2025] American Bureau of Shipping: ABS CyberSafety Program. URL: https://ww2.eagle.org/en/Products-and-Services/cyber/abs-cybersafety.html.

[ALK2021] Alkhadra, Rahaf; Abuzaid, Joud; AlShammari, Mariam; Mohammad, Nazeeruddin: Solar Winds Hack: In-Depth Analysis and Countermeasures: 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, Piscataway, NJ, 2021; S. 1–7.

[AMI2024] Amiri, Amirali; Steindl, Gernot; Gorton, Ian; Hollerer, Siegfried; Kastner, Wolfgang; Sauter, Thilo: Integrated Safety and Security by Design in the IT/OT Convergence of Industrial Systems: A Graph-Based Approach. In (Chang, R. N. Hrsg.): 2024 IEEE International Conference on Software Services Engineering. IEEE SSE 2024 Shenzhen, China, 7-13 July 2024 proceedings. IEEE, Piscataway, NJ, 2024; S. 123–129.

[ATU2025] Atug, Manuel: NIS2: Schulungspflicht für Geschäftsleitungen. In ix - Magazin für professionelle Informationstechnik, 4, 2025; S. 92–95. URL: https://www.wiso-net.de/browse/Alle%20Quellen/Fachzeitschriften/Elektroindustrie/iX%20-%20Magazin%20f%C3%BCr%20professionelle%20Informationstechnik?preview=IX__2025-4.

[BER2023] Berg, Achim: Wirtschaftsschutz 2023. URL: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf.

[BMI2024] Bundesministerium des Innern: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen. URL: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/KM4/regentwurf-kritisDachG.pdf?__blob=publicationFile&v=3.

[BMI2025] Bundesministerium des Innern: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen. Referentenentwurf, Bearbeitungsstand: 27.08.2025 16:26. URL: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/Kritis-Dachgesetz.pdf?__blob=publicationFile&v=1.

[BRE2024] Brenner, Michael; gentschen Felde, Nils; Hommel, Wolfgang; Metzger, Stefan; Reiser, Helmut; Schaaf, Thomas: Praxisbuch ISO/IEC 27001. Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. 5. Auflage. Hanser, München, 2024.

[BRO2011] Broad, William J.; Markoff, John, Sander, David E.: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&sq=stux.

[BSI_INF.13] Bundesamt für Sicherheit in der Informationstechnik (BSI): INF.13 Technisches Gebäudemanagement. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_13_Technisches_Gebaeudemanagement_Edition_2023.pdf?__blob=publicationFile&v=3.

[BSI_INF.13U] Bundesamt für Sicherheit in der Informationstechnik (BSI): Umsetzungshinweise zum Baustein INF.13 Technisches Gebäudemanagement. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweis_zum_Baustein_INF_13_Technisches_Gebaeudemanagement.pdf?__blob=publicationFile&v=2.

[BSI_INF.14] Bundesamt für Sicherheit in der Informationstechnik (BSI): INF.14 Gebäudeautomation. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_14_Gebaeudeautomation_Edition_2023.pdf?__blob=publicationFile&v=3.

[BSI_INF.14U] Bundesamt für Sicherheit in der Informationstechnik (BSI): Umsetzungshinweise zum Baustein INF.14 Gebäudeautomation. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweis_zum_Baustein_INF_14_Gebaeudeautomation.pdf?__blob=publicationFile&v=2.

[BSI100-4] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Standard 100-4 Notfallmanagement, 2008. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2.

[BSI2014] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, 12.01.2015.

[BSI2018a] Bundesamt für Sicherheit in der Informationstechnik: Anforderungen an netzwerkfähige Industriekomponenten. BSI-CS 067. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_067.pdf?__blob=publicationFile&v=1, 26.04.2025.

[BSI2018b] Bundesamt für Sicherheit in der Informationstechnik: Fallbeispiel Servicetechniker. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_095c.pdf?__blob=publicationFile&v=1, 25.07.2025.

[BSI2018c] Bundesamt für Sicherheit in der Informationstechnik: Empfehlung IT in der Produktion. Fallbeispiel Schwimmbad. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_095a.pdf?__blob=publicationFile&v=1, 23.07.2025.

[BSI2019] Bundesamt für Sicherheit in der Informationstechnik (BSI): Monitoring and Anomaly Detection in Production Networks. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_134E.pdf?__blob=publicationFile&v=1.

[BSI2021a] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Grundschutz: OPS.1.1.5: Protokollierung. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_5_Protokollierung_Edition_2021.pdf?__blob=publicationFile&v=2.

[BSI2021b] Bundesamt für Sicherheit in der Informationstechnik (BSI): IND.1: Prozessleit- und Automatisierungstechnik. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/08_IND_Industrielle_IT/IND_1_Prozessleit_und_Automatisierungstechnik_Edition_2021.pdf?__blob=publicationFile&v=2.

[BSI2022a] Bundesamt für Sicherheit in der Informationstechnik (BSI): IND.3.2 Fernwartung im industriellen Umfeld. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/08_IND_Industrielle_IT/IND_3_2_Fernwartung_im_industriellen_Umfeld_Edition_2022.pdf?__blob=publicationFile&v=3.

[BSI2022b] Bundesamt für Sicherheit in der Informationstechnik (BSI): Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2022. BSI-CS 005. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html;jsessionid=EEC337374A53B4720636D8C64B94EF99.internet081.

[BSI2022c] Bundesamt für Sicherheit in der Informationstechnik (BSI): Maßnahmenkatalog Ransomware. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.pdf?__blob=publicationFile&v=2.

[BSI2022d] Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden zur Reaktion auf IT- Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/Leitfaden_VP_VE.pdf?__blob=publicationFile&v=21.

[BSI2022e] Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheitsanalyse OPC UA. URL: https://cdn.weka-fachmedien.de/media_uploads/documents/1648647762-236-opcua-2022.pdf.

[BSI2023a] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1.

[BSI2023b] Bundesamt für Sicherheit in der Informationstechnik (BSI): Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen nach § 8 Abs. 1 Satz 1 BSIG. Version 2.0 vom 29.06.2023. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_2_0.pdf?__blob=publicationFile&v=3.

[BSI2024] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=6, 05.06.2014.

[BSI2025] Allianz für Cyber-Sicherheit: LARS ICS. Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Tools/LarsICS/LarsICS_node.html, 23.07.2025.

[BSI2025b] Bundesamt für Sicherheit in der Informationstechnik (BSI): Common Security Advisory Framework CSAF. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html.

[BSI-KritisV_2016]: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung). BSI-KritisV, 2016.

[BUN2017]: Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen

gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. NIS-UG: Bundesgesetzblatt, 2017.

[BUN2023]: Dritte Verordnung zur Änderung der BSI-Kritisverordnung. KritisV 2.0, 2023.

[CER_en]: Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. CER Richtlinie, 2022.

[CERT2016] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Cyber-Attack Against Ukrainian Critical Infrastructure. URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[CERT2018] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Alert (ICS-ALERT-14-176-02A). ICS Focused Malware (Update A). URL: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A, 20.07.2025.

[CHE2017] Cherepanow, Anton: Win32/Industroyer. A new threat for industrial control systems. URL: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.

[CHU2013] Chuvakin, A. Hrsg.: Logging and log management. The authoritative guide to understanding the concepts surrounding logging and log management. Syngress, Waltham, MA, 2013.

[CLA2024a] Claroty Ltd.: Remote Access Tool Sprawl. URL: https://web-assets.claroty.com/resource-downloads/claroty-team82-report_secure-access-tool-sprawl.pdf.

[CLA2024b] Claroty Ltd.: An Open Door. URL: https://web-assets.claroty.com/team82-secure-access-report.pdf.

[CRA2024] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). CRA, 2024.

[CYB2020] Cybersecurity & Infrastructure Security Agency: Ransomware Impacting Pipeline Operations Alert (AA20-049A). URL: https://www.us-cert.gov/ncas/alerts/aa20-049a.

[DHS2016] Department of Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. URL: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[DHS2025] Department of Homeland Security: Cybersecurity Alerts & Advisories. URL: https://www.cisa.gov/news-events/cybersecurity-advisories, 25.07.2025.

[DIR2015] DiRenzo, Joseph; Goward, Dana A.; Fred S. Roberts: The Little-known Challenge of Maritime Cyber Security: 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 2015.

[DNV2025] DNV AS: Cyber Secure class notation. URL: https://www.dnv.com/services/cyber-secure-class-notation-124600/.

[EIK2013] Eikenberg, Ronald: Vaillant-Heizungen mit Sicherheits-Leck. URL: http://www.heise.de/security/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html, 12.02.2016.

[ENI2025] ENISA European Union Agency for Network and Information Security: EU Vulnerability Database. URL: https://euvd.enisa.europa.eu/search.

[ENN2021] Ennenbach, Martin et al.: Leitfaden Cyber-Sicherheits-Check OT. Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks der operativen Technologie (CSC-OT) in der Industrie und Automatisierungstechnik. URL: https://www.isaca.de/sites/default/files/isaca_leitfaden_cyber-sicherheits-check_ot.pdf.

[EUR2006]: Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung). Maschinenrichtlinie, 2006.

[FAL2011] Falliere, Nicolas; Murchu, Liam O.; Chien, Eric: W32.Stuxnet Dossier. URL: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en, 21.08.2014.

[FLU2022] Fluchs, Sarah; Tasten, Emre; Mertens, Martin; Horch, Alexander; Drath, Rainer; Fay, Alexander: Security by Design Integration Mechanisms for Industrial Control Systems: IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2022; S. 1–6.

[FOR2025] Fortinet Inc.: Solar-Winds Cyber Angriff. URL: https://www.fortinet.com/de/resources/cyberglossary/solarwinds-cyber-attack.

[GAN2023] Ganschowr, Sebastian: Stolperfallen vermeiden, Sicherheit erhöhen. IT- und OT-Integration. In Industrie 4.0 Magazin, 7, 2023; S. 11–12.

[GRA2024] Graham, Mark; Ahlers; Carolyn; o' Meara, Kyle: Impact of FrostyGoop ICS Malware on Connected OT Systems. URL: https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_.pdf.

[HÄU2023] Häußler, Alexander: ISO/IEC 27001 Information security management system and the road to certification. URL: https://www.tuvsud.com/en/resource-centre/white-papers/iso-iec-27001-information-security-management.

[HÜN2024] Hüning, Alois; Reusch, Philipp; Gast, Torsten: Die neue EU-Maschinenverordnung. Übersicht über die Änderungen, Lösungen und Antworten für die Praxis. Vogel Communications Group, Würzburg, 2024.

[ICS2025] ICS-CERT: Downloading and Installing CSET. URL: https://www.cisa.gov/downloading-and-installing-cset, 23.07.2025.

[IEC_62443-1-1] International Electrotechnical Commission, IEC/TS 62443-1-1:2009: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, 2009. URL: https://webstore.iec.ch/publication/7029.

[IEC_62443-1-2] IEC- International Electrotechnical Commission, ISA-TR62443-1-2: Security for industrial automation and control systems - Master Glossary - Draft not publicly available. URL: http://isa99.isa.org/Public/Documents/ISA-62443-1-2-WD.pdf.

[IEC_62443-1-3] IEC- International Electrotechnical Commission, IEC/TS 62443-1-3: Security for industrial process measurement and control – Network and system security – Part 1-3: System security compliance metrics - Draft not publicly available, 2014. URL: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[IEC_62443-1-4] IEC- International Electrotechnical Commission, ISA-62443-1-4: Security for industrial automation and control systems Life Cycle and Use Cases - Draft - Not publicly available, 2013. URL: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[IEC_62443-1-5] IEC- International Electrotechnical Commission, IEC TS 62443-1-5: Security for industrial automation and control systems - Part 1-5: Scheme for IEC 62443 security profiles, 2023. URL: https://webstore.iec.ch/publication/67461.

[IEC_62443-2-1] International Electrotechnical Commission, IEC 62443-2-1:2024: Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners, 2024. URL: https://www.vde-verlag.de/iec-normen/254227/iec-62443-2-1-2024.html.

[IEC_62443-2-2] IEC- International Electrotechnical Commission, IEC 62443-2-2:2025: Security for industrial automation and control systems – Part 2-2: IACS security protection scheme, 2025. URL: https://www.vde-verlag.de/iec-normen/254909/iec-pas-62443-2-2-2025.html.

[IEC_62443-2-4] IEC- International Electrotechnical Commission, IEC 62443-2-4:2023: Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers, 2023. URL: https://webstore.iec.ch/en/publication/67631.

[IEC_62443-3-1] IEC- International Electrotechnical Commission, IEC TR 62443-3-1:2009: Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems, 2009.

[IEC_62443-3-2] IEC- International Electrotechnical Commission, IEC 62443-3-2:2020: Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design, 2020. URL: https://webstore.iec.ch/en/publication/30727.

[IEC_62443-3-3] IEC- International Electrotechnical Commission, IEC 62443-3-3:2013: Security for industrial automation and control systems Part 3-3: System security requirements and security levels, 2013. URL: https://webstore.iec.ch/en/publication/7033.

[IEC_62443-4-1] IEC- International Electrotechnical Commission, IEC 62443-4-1: Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements, 2018.

[IEC_62443-4-2] IEC- International Electrotechnical Commission, IEC 62443-4-2: Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components, 2019.

[IEC_62443-6-1] IEC- International Electrotechnical Commission, IEC TS 62443-6-1:2024: Security for industrial automation and control systems - Part 6-1: Security evaluation methodology for IEC 62443-2-4, 2024. URL: https://www.vde-verlag.de/iec-normen/252700/iec-ts-62443-6-1-2024.html.

[IEC_62443-6-2] IEC- International Electrotechnical Commission, IEC TS 62443-6-2:2025: Security for industrial automation and control systems - Part 6-2: Security evaluation methodology for IEC 62443-4-2, 2025. URL: https://www.vde-verlag.de/iec-normen/254715/iec-ts-62443-6-2-2025.html.

[IEC_62451-2] IEC- International Electrotechnical Commission, IEC TR 62541-2:2020 RLV: OPC unified architecture - Part 2: Security Model, 2020. URL: https://webstore.iec.ch/publication/68036.

[IEC_TR_62443-2-3] IEC- International Electrotechnical Commission, IEC TR 62443-2-3:2015: Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment, 2015. URL: https://webstore.iec.ch/en/publication/22811.

[IMO2017] International Maritime Organization (IMO): Resolution MSC.428(98) (adopted on 16 June 2017) Maritime Cyber Risk Management in Safety Management Systems. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

[IMO2025] International Maritime Organization (IMO): Guidelines on Maritime Cyber Risk Management. MSC-FAL.1/Circ.3/Rev.3. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf.

[ISE2025] IsecT Ltd: Overwiew on ISO 27000 standard series. URL: https://www.iso27001security.com/html/iso27000.html.

[ISO/IEC_27006-1] ISO - International Standardization Organization, ISO/IEC 27006-1:2024: Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems, Part 1: General, 2024. URL: https://www.iso.org/standard/82908.html.

[ISO_27000] ISO - International Standardization Organization, ISO/IEC 27000:2018(E): Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2018.

[ISO_IEC_27001] International Organization for Standardization (ISO), ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements, 2022. URL: https://www.iso.org/standard/82875.html.

[ISO_IEC_27002] International Organization for Standardization (ISO), ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/standard/75652.html.

[IT_SIG_2.0]: Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0). IT-SiG 2.0: Bundesgesetzblatt, 2021; S. 1122–1138.

[ITSichG2015] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015.

[JEN2015] Jensen, Lars: Challenges in Maritime Cyber-Resilience. In Technology Innovation Management Review, 04, 2015; S. 35–39. URL: http://timreview.ca/sites/default/files/article_PDF/Jensen_TIMReview_April2015.pdf.

[KAL2024] Kallisch, Jonas; Niemann, Karl-Heinz; Wunck, Christoph: Bridging the Data Borders – Connecting Supply-Chain Shop-Floors. In (Witte, P.; Niemann, Karl-Heinz Hrsg.): Sensorik und Automation: Schriften des Forschungsinstituts ISA 2024. HsH Applied Academics, 2024; S. 50–61. https://doi.org/10.25968/opus-3245.

[KAL2025] Kallisch, Jonas; Voss, Marvin; Runge, Maxim; Wunck, Christoph; Niemann, Karl-Heinz: Cyber-Sicherheit in vernetzten Lieferketten. 441 KB, 2025. URL: https://doi.org/10.25968/opus-3594.

[KIR2022] Kirketerp de Viron, Christiane; Stefanuc, Raluca; Boegel, Benjamin; Fohrenbach, Maika: Cyber Resilience Act: new EU cybersecurity rules ensure safer hardware and software, Connect University Online Session, 2022.

[KOB2021] Kobes, Pierre: Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments. URL: https://gca.isa.org/blog/white-paper-excerpt-applying-iso/iec-27001/2-and-the-isa/iec-62443-series-for-operational-technology-environments.

[KOB2023] Kobes, Pierre: Guideline industrial security. IEC 62443 is easy. VDE Verlag GmbH, Berlin, 2023.

[KUI2006] Kuipers, David; Fabro, Mark: Control Systems Cyber Security:Defense in Depth Strategies. URL: https://www.osti.gov/biblio/911553.

[LAN2013] Langner, Ralph: To kill a centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. URL: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, 13.11.2014.

[LAN2022] Langreder, Philipp; Schmidt, Frank; Niemann, Karl-Heinz: Fernwartung und OT-Security. In atp magazin, 9, 2022; S. 64–73. URL: https://doi.org/10.25968/opus-2366.

[LEL2021] Lella, Ifigeneia; Theocharidou, Marianthi; Tsekmezoglou, Eleni; Malatras, Apostolos: ENISA Threat Landscape for Supply Chain Attacks. URL: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

[LI2023] Li, Guowen; Ren, Lingyu; Fu, Yangyang; Yang, Zhiyao; Adetola, Veronica; Wen, Jin; Zhu, Qi; Wu, Teresa; Candan, K.Selcuk; O'Neill, Zheng: A critical review of cyber-physical security for building automation systems. In Annual Reviews in Control, 2023, Jahrgang 55; S. 237–254.

[LLO2024] Lloyd's Register: Digital Ships Procedures. URL: https://www.lr.org/en/knowledge/lloyds-register-rules/shipright/digital-ships/.

[MIC2023] Microsoft: Microsoft Threat Modeling Tool. URL: https://learn.microsoft.com/de-de/azure/security/develop/threat-modeling-tool, 23.07.2025.

[MIT2025a] Mitre Corporation: Common Vulnerabilities and Exposures. URL: https://www.cve.org/, 25.07.2025.

[MIT2025b] Mittelstand Digital: SiToM - Sicherheitstool Mittelstand. URL: https://www.sitom.de/home.

[NA_115_en] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V: IT-Security for Industrial Automation IT Security for Industrial Automation Systems - Constraints for measures applied in process industries, 17.11.2016.

[NA_163_en] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NA 163: IT Security Risk Assessment for Safety-Related PCT Equipment, 2024.

[NA_169_en] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NA 169: Automation Security Management in the Process Industry, Leverkusen, 2019.

[NE_135_en] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 135: Remote Access - Requirements for remote access security, Leverkusen, Version: 2023. URL: https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html.

[NE_153_en] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 153: Automation Security 2020 – Design, Implementation and Operation of Industrial Automation Systems, Leverkusen, 2015.

[NE_177] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 177: NAMUR Open Architecture - NOA Security Zonen und NOA Security Gateway, 2021. URL: https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html.

[NE_193] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 193: Ein Informationsmodell für das Automation Security Engineering, 2024.

[NE_201_en] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 201: Identity and Access Management on Automation Devices, 2025. URL: https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html.

[NHL2025] NHL Stenden - University of Applied Sciences: MCAD Maritime Cyber Attack Database. URL: https://maritimecybersecurity.nl/.

[NIE2014a] Niemann, Karl-Heinz: IT-Security-Konzepte für die Prozessindustrie. Anforderungen im Kontext von Industrie 4.0. In atp-edition, 7-8/2014, 2014, Jahrgang 56; S. 62–69. URL: http://media.di-verlag.de/atp/atp_07-08_2014_Niemann.pdf.

[NIE2014b] Niemann, Karl-Heinz: IT Security Konzepte. Anforderungen im Kontext von Industrie 4.0. In (VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik Hrsg.): Automation 2014. Smart X - Powered by Automation. VDI-Verlag GmbH, Düsseldorf, 2014; S. 489–506.

[NIE2021] Niemann, Karl-Heinz: Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443 - Eine Sicht auf automatisierungstechnische Anlagen der Fertigungs- und Prozessindustrie. URL: https://doi.org/10.25968/opus-1973.

[NIE2023a] Niemann, Karl-Heinz; Walz, Andreas; Sikora, Axel: Security Extensions for PROFINET. Concepts, Status, and Prospects. In (Sikora, A. Hrsg.): Embedded World Conference 2023 Proceedings. WEKA Fachmedien GmbH, 2023; S. 99–104.

[NIE2023b] Niemann, Karl-Heinz; Walz, Andreas; Merklin, Simon; Ziegler, Andreas; Waldeck, Boris: How to develop a secure PROFINET device. Organizational and technical OT security measures during the development of PROFINET devices. Englisch Translation of German article. In atp Magazin, 2023; S. 62–70. URL: https://doi.org/10.25968/opus-3036.

[NIE2024a] Niemann, Karl-Heinz; Göppert, Julian; Walz, Andreas; Ziegler, Dominik: Security-Event-Logging am Beispiel von PROFINET. In (Technische Hochschule Ostwestfalen-Lippe; Jasperneite, Jürgen; Jumar, Ulrich Hrsg.): Kommunikation in der Automation Beiträge des Jahreskolloquiums KommA 2024. Institut für industrielle Informationstechnik - inIT der Technischen Hochschule Ostwestfalen-Lippe, 2024; S. 48–60. https://doi.org/10.25644/jnac-vp34.

[NIE2024b] Niemann, Karl-Heinz; Kobes, Pierre: ISO 27000 oder IEC 62443? Wie man beide Normreihen sinnvoll für die OT-Security kombiniert. In atp Magazin, 03, 2024; S. 60–67. URL: https://doi.org/10.25968/opus-3072.

[NIS1_en] Directive (EU) 2016/1148 of the European Parliarment and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016.

[NIS2_DE_2025]: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Drucksache 21/1501, 2025.

[NIS2_en] Directive (EU) 2022/2555 of the European Parlinament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive): Official Journal of the European Union, 2022; S. 80–152.

[ODV2023] ODVA Inc.: Overview of CIP Security. URL: https://www.odva.org/wp-content/uploads/2023/07/PUB00319R2_CIP-Security-At-a-Glance.pdf.

[OTO2022] OTORIO Ltd.: 2022 OT Cybersecurity Survey Report. URL: https://go.otorio.com/hubfs/Whitepapers%20and%20Reports/OTORIO_2022%20OT%20Cybersecurity%20Survey%20Report.pdf.

[PAK2005] Pakalski, Ingo: Computerwurm befällt CNN, DaimlerChrysler und Walt Disney. URL: http://www.golem.de/0508/39902.html.

[PAN2008] Pany, Thomas: Saboteur schaltet Turbine des britischen Kohlekraftwerks Kingsnorth aus. URL: https://www.heise.de/newsticker/meldung/Saboteur-schaltet-Turbine-des-britischen-Kohlekraftwerks-Kingsnorth-aus-188799.html?view=print.

[PIT2023] Pittler, Jens: Sabotageaufklärung in Logistikunternehmen. URL: https://rhebo.com/de/download/file/case-study-sabotageaufklaerung-im-logistikunternehmen/.

[PNO2013] PROFIBUS Nutzerorganisation e.V.: PROFINET Security Guideline. URL: https://www.profibus.com/download/profinet-security-guideline.

[PNO2019] PROFIBUS Nutzerorganisation e.V.: Security Extensions for PROFINET. PI White Paper for PROFINET. URL: https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/.

[PNO2022] PROFIBUS Nutzerorganisation e.V.: OT security for production plants with PROFINET. A classification of IEC 62443 for operators, integrators and manufacturers. URL: https://www.profibus.com/download/white-paper-ot-security-classification-of-iec62443.

[PNO2023] PROFIBUS Nutzerorganisation e.V.: Security Class 1 for PROFINET-Security Guideline for PROFINET. URL: https://www.profibus.com/download/profinet-security-guideline.

[PON2017] Ponemon Institute LLC: 2017 Cost of Data Breach Study. URL: https://www.ponemon.org/news-updates/blog/security/2017-cost-of-data-breach-study-united-states.html.

[PUL2024a] Puls, Jan-Niklas; Niemann, Karl-Heinz: Einführen eines Informationssicherheitsmanagementsystems in einem KMU. In Zukunft.Digital, 02, 2024; S. 26–29. URL: https://digitalzentrum-hannover.de/wp-content/uploads/2024/12/MDZH_Magazin_24-02_web.pdf.

[PUL2024b] Puls, Jan-Niklas; Niemann, Karl-Heinz; Meyer, Sebastian: Best Practice zu Verschlüsselungstrojaner-resilienten Datensicherungen. URL: https://doi.org/10.25968/opus-3095.

[SAN2015] SANS Institute: The State of Security in Control Systems Today. URL: http://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042, 19.07.2016.

[SAN2016] SANS Institute: Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf.

[SCH2018] Scherschel, Fabian A.: Nach NotPetya-Angriff: Weltkonzern Maersk arbeitete zehn Tage lang analog. URL: https://www.heise.de/newsticker/meldung/Nach-NotPetya-Angriff-Weltkonzern-Maersk-arbeitete-zehn-Tage-lang-analog-3952112.html.

[SEC2024] Securitons: Das KRITIS-Dachgesetz und seine Umsetzung. URL: https://www.securiton.de/fileadmin/user_upload/Dokumente_PDFs/Downloads/Whitepaper/KRITIS-Dachgesetz/Whitepaper_KRITIS_Dachgesetz_Securiton_112024.pdf.

[SIE2025] Siemens Aktiengesellschaft: ProductCERT Security Advisories. URL: http://www.siemens.com/cert/de/cert-security-advisories.htm, 29.11.2016.

[STA2013] Stahl, Louis-F.; Eikenberg, Ronald: Fünf nach zwölf. Die „Gefahr im Kraftwerk" ist noch nicht gebannt. In c't Magazin für Computertechnik, 15, 2013; S. 16–17.

[STA2025a] Statista GmbH: Anzahl der umsatzsteuerpflichtigen Unternehmen in Deutschland von 2004 bis 2023. URL: https://de.statista.com/statistik/daten/studie/246358/umfrage/anzahl-der-unternehmen-in-deutschland/.

[STA2025b] Statista GmbH: Bestand an gültigen ISO-27001-Zertifikaten in Deutschland in den Jahren 2006 bis 2023. URL: https://de.statista.com/statistik/daten/studie/829353/umfrage/bestand-an-vergebenen-iso-27001-zertifikaten-in-deutschland/.

[STE2019] Steinke, Kai; Tebbje, Sebastian; Niemann, Karl-Heinz: Änderung von IT-Security-Anforderungen durch den Wandel der Automatisierungsstrukturen im Kontext von Industrie 4.0. In (Bauer, B.; Wittenberg, Carsten Hrsg.): Tagungsband AALE 2019. 16. Fachkonferenz, Autonome und intelligente Systeme in der Automatisierungstechnik, 2019; S. 97–104.

[TOF2009] Tofino Security: Daimler Chrysler Cyber Security Incident case Profile. Virus shuts down 13 plants; loss estimated at $14 million. URL: https://www.tofinosecurity.com/sites/default/files/CP-104-Case_Profile-Daimler_Chrysler-rev1.pdf.

[TÜV2025] TÜV Verband: TÜV Cybersecurity Studie 2025 - Cybersicherheit in deutschen Unternehmen. Neue Bedrohungslage – besserer Schutz. URL: https://www.tuev-verband.de/fileadmin/user_upload/Content_local/Studien_local/2025_TUEV-Verband_Cybersecurity-Studie_Studienbericht.pdf.

[UR_E26] International Association of Classification Societies (IACS), UR E26 REV1 CR: Cyber resilience of ships, 2023. URL: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf.

[UR_E27] International Association of Classification Societies (IACS), UR E27 Rev. 1: Cyber resilience of on-board systems and equipment, 2023. URL: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf.

[VDI_2182_1_en] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Part 1: IT-security for industrial automation - General model. Beuth Verlag, Berlin, 2020. URL: https://www.dinmedia.de/de/technische-regel/vdi-vde-2182-blatt-1/314114388.

[VDI_2182_2_1_en] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Part 2.1: IT-security for industrial automation Example of use of the general model for device manufacturer in factory automation Programmable logic controller (PLC). Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-21/170847294?SearchID=889635358.

[VDI_2182_2_2_en] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Part 2.2: IT-security for industrial automation Example of use of the general model in factory automation for plant and machinery installers - Forming press. Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-22/173513663?SearchID=889639460.

[VDI_2182_2_3_en] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182, Part 2.3: IT security for industrial automation Example of use of the general model for plant managers in factory automation - Stamping plant. Beuth Verlag, Berlin, 2017.

[VDI_2182_3_1_en] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Part 3.1: IT-security for industrial automation Example of use of the general model for manufacturers in process automation Process control system of an LDPE

plant. Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-31/187310424?SearchID=890274896.

[VDI_2182_3_2_en] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Part 3.2: IT-security for industrial automation Example of use of the general model for integrators in process industry - LPDE reactor. Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-32/167996669?SearchID=890279216.

[VDI_2182_3_3_en] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Part 3.3: IT-security for industrial automation Example of use of the general model for plant managers in process industry - LDPE-plant. Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-33/170881034.

[VDM2023] VDMA - Verband der Maschinen und Anlagenbauer e. V.: VDMA Lastenheft Supply Chain Security. Betreiber - Integrator. URL: https://www.vdma.org/documents/34570/14530044/SuD_2023-01+VDMA+Supply+Chain+Security+Lastenheft_Datei.pdf.

[VDS_10000] VdS Schadenverhütung GmbH, VdS 10000:2025-01(03): Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), 2025. URL: https://shop.vds.de/publikation/vds-10000.

[VDS_10020] VdS Schadenverhütung GmbH, VdS 10020:2020-04(02): Cyber Security für kleine und mittlere Unternehmen (KMU) - Leitfaden zur Interpretation und Umsetzung der VdS 3473 für Industrielle Automatisierungssysteme, Köln, 2018.

[VIS2020] Visoky, Jack; Wiberg, Joakim: CIP Security and IEC 62443-4-2. URL: https://www.odva.org/wp-content/uploads/2020/05/2020-ODVA-Conference_CIP_Security_and_IEC_62443_Visoky_Wiberg_Final.pdf.

[VOß2024] Voß, Marvin; Kallisch, Jonas; Runge, Maxim; Theus, Tobias; Niemann, Karl-Heinz; Wunck, Christoph: IT-Security Risk Based Approach for Secure Operation of Distributed Data Platforms in Supply Chains: 2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE, 2024; S. 952–958.

[WAG2025] WAGO Kontakttechnik GmbH & Co. KG: Wago Security-Hinweise Automatisierungskomponenten über VDE-CERT. URL: https://www.wago.com/de/automatisierungstechnik/security, 31.07.2018.

[WAL2023] Walz, Andreas; Niemann, Karl-Heinz; Göppert, Julian; Fischer, Kai; Merklin, Simon; Ziegler, Dominik; Sikora, Axel: PROFINET Security: A Look on Selected Concepts for Secure Communication in the Automation Domain: 2023 IEEE 21st International Conference on Industrial Informatics (INDIN). IEEE, 2023 - 2023; S. 1–6.

[WUL2022] Wulfmeier, Kirsten; Niemann, Karl-Heinz: Befragung zur Auswertung von Security Advisories im Produktionsumfeld durch KMU. URL: https://doi.org/10.25968/opus-2303.

[ZET2016] Zetter, Kim: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. URL: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 05.03.2016.