

IEC 62443 from the planner's and operator's point of view

Karl-Heinz Niemann

Suggested citation:

Niemann, Karl-Heinz. 2025. "IEC 62443 from the planner's and operator's point of view."
Hannover: Hochschule Hannover. <https://doi.org/10.25968/opus-3739>.

Abstract

IT security in production plants is becoming increasingly important. Statistics confirm a deteriorating threat situation in the field of industrial automation technology. In future, the European Union will require certain minimum standards for systems in critical infrastructure and other areas via the NIS2 Directive. Planners and operators of production facilities are therefore required to address the IT security of their production facilities (hereinafter referred to as OT security) and systematically integrate it into their processes.

The IEC 62443 series of standards was designed specifically for use in production plants and therefore considers the requirements for industrial real-time environments. In addition to requirements for manufacturers of automation components, the standard also defines requirements for planners and operators of automation systems. This document focuses on the role of planners and operators in the OT security process.

After a differentiation between OT security and IT security in chapter 2, an introduction to the IEC 62443 standard follows in chapter 3. Chapter 4 then describes the tasks of the system planner. Among other things, the tasks of the system planner, such as the creation of a risk and threat analysis and the definition of a defense-in-depth concept, are discussed here. This is followed in chapter 5 by the tasks of the asset owner. These tasks include, for example, setting up an information security management system (ISMS), creating and maintaining an asset inventory and installing software updates (patch management).

WHITE PAPER

IEC 62443 from the planner's and operator's point of view

Prof. Dr. Karl-Heinz Niemann



Prof. Dr. Karl-Heinz Niemann


ORCID ID  <https://orcid.org/0000-0001-8931-6789>

ABB document number: 3ADR011430, 1, en_US

DOI: [10.25968/opus-3739](https://doi.org/10.25968/opus-3739)

Disclaimer: The information on which this document is based has been compiled with the greatest possible care. Nevertheless, it is provided without warranty of any kind. The author expressly disclaims 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.

Version history

Rev.	Version Description	Date
C	First published version	27.07.2025
C3	Translation to English	26.09.2025
D	Finalization of the English version of the document	26.10.2025

Contents

1. Introduction	5
2. Differentiation between OT and IT security	6
3. The IEC 62443 series of standards	7
3.1. Overview of IEC 62443	7
3.2. The roles in the OT security process	8
3.3. Interaction of stakeholders in the OT security process	9
3.4. The security levels in IEC 62443	10
4. The tasks of the system planner according to IEC 62443	12
4.1. Relevant parts of the IEC 62443 standard for system planners	12
4.2. The tasks of the system planner in detail	13
4.2.1. Identification of existing documents of the client / system operator	13
4.2.2. Definition of the object under consideration (system under consideration)	14
4.2.3. Definition of the security context	14
4.2.4. Risk and threat analysis	15
4.2.5. Defense in Depth Concept	17
4.2.6. Creating the detailed planning	19
4.2.7. Results of the planning process	19
4.3. Interaction of the planner with the other responsible parties in the OT security process	20
4.4. Proposal for the realization of the security requirements	20
4.5. Success factors for the OT security process of system planners	21
5. The tasks of the system operator according to IEC 62443	22
5.1. Relevant parts of the IEC 62443 standard for system operators	22
5.2. The tasks of the system operator in detail	24
5.3. Cooperation with the other responsible parties in the OT security process	25
5.4. Proposal for a procedure for implementing the requirements for operators	25
5.5. Success factors for the security process of plant operators	26
6. Summary	27
7. List of figures	28
8. List of tables	29
9. Index	30
10. Bibliography	32

1. Introduction

IT security in production plants is becoming increasingly important. Statistics confirm a deteriorating threat situation in the field of industrial automation technology [TRE2022]. In future, the European Union will require certain minimum standards for systems in critical infrastructure and other areas via the NIS2 Directive [NIS2_en]. Planners and operators of production facilities are therefore required to address the IT security of their production facilities (hereinafter referred to as OT security) and systematically integrate it into their processes.

The IEC 62443 [ISA2025] series of standards was designed specifically for use in production plants and therefore considers the requirements for industrial real-time environments. In addition to requirements for manufacturers of automation components, the standard also defines requirements for planners and operators of automation systems. This document focuses on the role of planners and operators in the OT security process.

After a differentiation between OT security and IT security in chapter 2, an introduction to the IEC 62443 standard follows in chapter 3. Chapter 4 then describes the tasks of the system planner. Among other things, the tasks of the system planner, such as the creation of a risk and threat analysis and the definition of a defense-in-depth concept, are discussed here. This is followed in chapter 5 by the tasks of the asset owner. These tasks include, for example, setting up an information security management system (ISMS), creating and maintaining an asset inventory and installing software updates (patch management). The document concludes with a summary.

Wherever possible, references are made to further literature sources. The list of sources can be found in the bibliography in chapter 10.

2. Differentiation between OT and IT security

In the area of information security, a distinction is made between IT (Information Technology) and OT (Operational Technology). The Gartner Group [GAR2021] differentiates between IT and OT according to the characteristics listed in Table 1.

Table 1: Differentiation between IT and OT according to [GAR2021]

Domain	Definition according to the Gartner Group	Application example
IT	"IT" (Information Technology) is the common term for the entire spectrum of technologies for information processing, including software, hardware, communication technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.	<ul style="list-style-type: none"> • Workstations • Laptops • Web servers • Mail servers • SAP systems • File servers • Networks
OT	Operational Technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.	<ul style="list-style-type: none"> • Programmable logic controllers (PLC) • Display systems (operator panels) • Servers for production control • Industrial robots • Remote IO systems • Real-time networks and other networks for communication with automation components.

Operational Technology (OT) essentially refers to automation technology components. The special requirements of OT are:

- Real-time communication is essential for the functionality of an automation system and therefore for the production plant.
- In the process industry continuous, uninterrupted operation of the systems must be assumed.
- It is only possible to install software patches during operation of the system to a limited extent.
- Communication integrity protection is required.
- Fulfillment of the essential safety requirements:
 - Availability
 - Integrity
 - Authenticity
 - Confidentiality
 - Non-repudiation

These requirements mean that certain aspects of OT security (e.g. patch management) must be handled differently than in IT. In principle, however, there are also many similarities, e.g. in the establishment and maintenance of an Information Security Management System (ISMS).

3. The IEC 62443 series of standards

The following chapter is dedicated to the IEC 62443 series of standards [ISA2025]. Chapter 3.1 begins with an overview of the standard. Chapter 3.2 then deals with the roles in the OT security process. This is followed by a description of the interaction of the stakeholders in the OT security process in chapter 3.3.

3.1. Overview of IEC 62443

The IEC 62443 series of standards covers the security (OT security) in the field of automation technology (Industrial Automation and Control Systems – IACS). The series of standards addresses the components that are required for the operation of an automated production system. This includes both hardware and software components. Furthermore, the organizational processes for the installation and operation of a control system are also included.

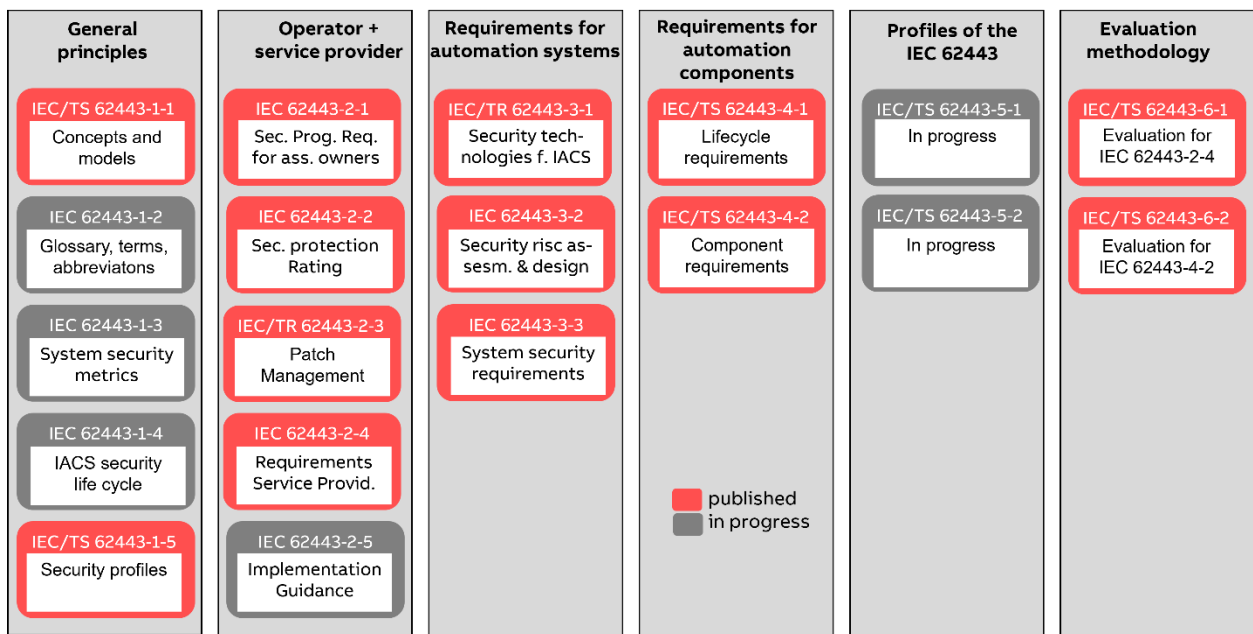


Figure 1: Overview of the IEC 62443 series of standards, based on [DKE2024]

Figure 1 provides an overview of the IEC 62443 series of standards. The series can be divided into four main categories:

- **Parts 1-1 to 1-5 - General principles:** these documents define the terms and principles related to OT security. Currently, only Part 1-1 and Part 1-5 are publicly available.
- **Parts 2-1 to 2-5 - Operators and service providers:** These parts are relevant for system operators and service providers. These parts define, for example, the security management process, guidelines for patch management and requirements for service providers (e.g. maintenance personnel). Part 2-2 also deals with the classification of technical security features and the maturity level of the organization. The Parts 2-1 to 2-5 of the standard will be discussed in more detail in the chapters 4 and 5 of this document, which deals with the tasks of integrators and system operators.

- **Parts 3-1 to 3-3 - Requirements for automation systems:** These parts are important for the planning of an automation system. They provide information on the risk management process (Part 3-2) and on the requirements for system security (Part 3-3). These parts are relevant to chapter 4 of this document, which deals with the process of designing a system securely.
- **Parts 4-1 to 4-2 - Requirements for automation components:** These two parts define the secure development life cycle for automation components (Part 4-1) and the technical requirements for automation components (Part 4-2). These two parts are relevant for manufacturers of components for automation systems and are therefore not considered in detail here.
- **Parts 5-1 and 5-2:** These parts are not yet available. It is planned to describe profiles that support the application of the standard in different areas, e.g. industrial automation, process industry, medical or railroad technology.
- **Parts 6-1 and 6-2 - Evaluation methodology:** These two parts describe conformity criteria and possible proofs of conformity. No new requirements are defined, but it is described how conformity with the requirements of the IEC 62443 standard can be evaluated. Part [IEC_62443-6-1] deals with the evaluation methodology for service providers, part [IEC_62443-6-2] with the evaluation of the requirements for automation components.

In addition to the OT security standard IEC 62442, the ISO 27000 series of standards is also frequently used in relation to security. While IEC 62443 focuses on OT security, [ISO_IEC_27001] deals with general aspects of information security. Anyone interested in the areas of application and the differences can find further information in the white paper "Differentiation of the IT security standard series ISO 27000 and IEC 62443" [NIE2021]. In addition to the standards described, further documentation on OT security is available, e.g. in the NIST "Guide to Operational Technology (OT) Security" [NIST_SP_800-82].

3.2. The roles in the OT security process

[IEC_62443-4-1] defines various stakeholders in the security management process. These are:

- **System operators and service providers** who support the system operator in operating the system. These can be companies who carry out maintenance tasks, for example.
- **System integrators and automation system planners** who design, install and commission automation systems and production facilities.
- **Product and system suppliers**, who develop and distribute components of automation systems as well as complete automation systems and supply the systems with updates and the operators with security advisories.

Figure 2 shows the various players and their role in the OT security process. The parts of IEC 62443 that are relevant for the respective stakeholders are listed on the right-hand side of Figure 2.

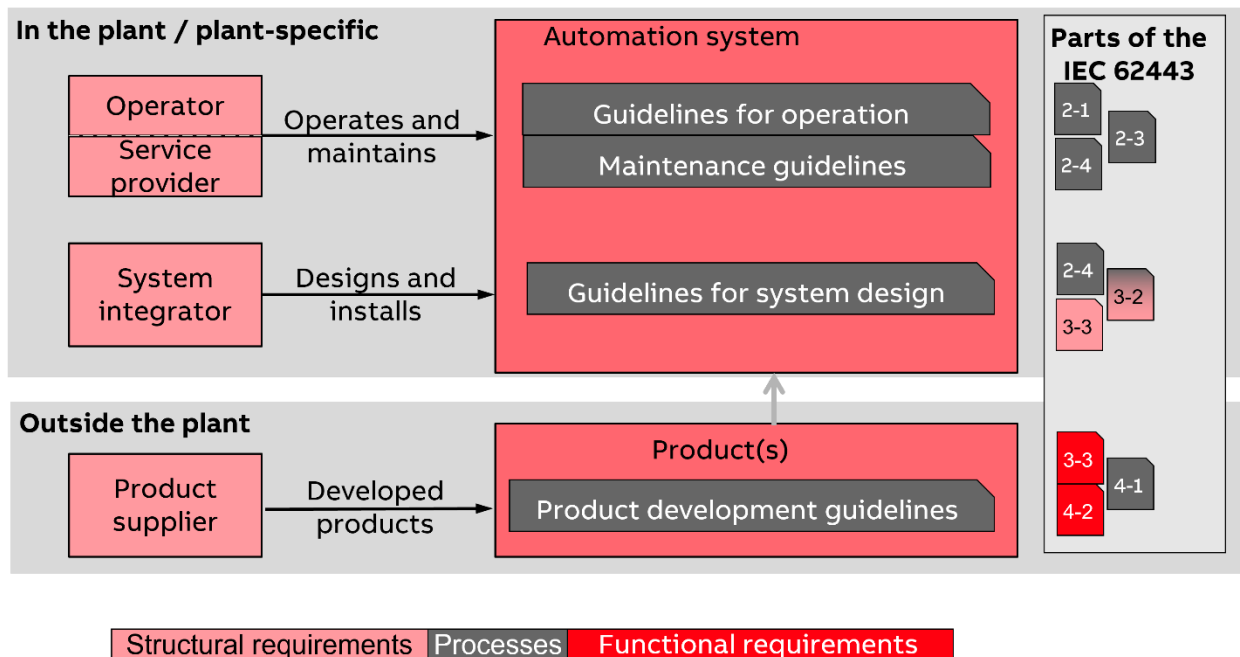


Figure 2: Stakeholders in the OT security process and assigned parts of IEC 62443 (derived from [IEC_62443-4-1])

3.3. Interaction of stakeholders in the OT security process

It can be seen in Figure 2 that various parts of IEC 62443 are relevant for the different stakeholders. It is assumed that the production plant under consideration should comply with the requirements of IEC 62443. Therefore, the term "must" will be used in the following text. Overall security is only guaranteed if the partial services for manufacturing the components, planning and constructing the system and operating it comply with the standard.

- **Plant operator:** The plant operator focuses on setting up the industrial security program in accordance with [IEC_62443-2-1] in his plant and classifies the level of maturity achieved in accordance with [IEC_62443-2-2]. He must plan and monitor patch management [IEC_TR_62443-2-3] and must define and monitor the security requirements for service providers (e.g. service, maintenance and commissioning personnel) working in the system in accordance with [IEC_62443-2-4].
- **System integrator:** The system integrator / system planner designs, installs and commissions automation systems. If the system integrator works as a contractor, he must comply with the security rules for service providers in accordance with [IEC_62443-2-4]. As part of the planning process, a risk assessment of the automation system must be carried out in accordance with [IEC_62443-3-2]. This task is usually carried out in cooperation / with the support of the system operator. During planning, the system integrator must observe the system security requirements defined in [IEC_62443-3-3].
- **Product supplier:** The product supplier must be familiar with the system-wide security requirements in accordance with [IEC_62443-3-3], as the component requirements were derived from this standard. The supplier must qualify his R&D and product management organization in accordance with [IEC_62443-4-1]. Product-specific requirements relating to the automation components are defined in [IEC_62443-4-2].

The various parties involved must comply with the processes defined in IEC 62443 in their area of responsibility and fulfill the requirements to produce compliant components and systems within the scope of IEC 62443.

The role of the product supplier is not considered further in the rest of the document.

3.4. The security levels in IEC 62443

The security levels are defined in [IEC_62443-3-3]. The standard recognizes three types of security levels (SL): security level to be achieved (target security level), security level achieved and achievable security level (Capability SL). These three types relate to the different phases of the secure development lifecycle.

- The **Target SL** (SL-T) describes the desired security level of a system. The SL-T is usually defined as part of the risk assessment. The security context and the threats posed by the environment of the system play a role here.
- The **Achieved SL** (SL-A) defines the achieved security level of the system under consideration. This can be determined after the system has been specified and after the system has been implemented. By determining the SL-A, it is possible to determine whether a system fulfills the requirements defined in the SL-T.
- The **Capability SL** (SL-C) (achievable SL) is the security level that a component or system can deliver if configured correctly. The SL-C indicates that a specific component or system can achieve the target SL (SL-T) on its own without additional measures if it is configured and integrated correctly.

The SLs described above are applied in the various phases of the OT security lifecycle. Starting with the target for a given system, the operator and/or system integrator will create a design for the automation system based on the requirements of the process to be automated and its potential risk to personnel and the environment. A specification for the SL-T is created on this basis. The system is then designed in such a way that the desired SL-T can be achieved. This is often an iterative process in which the achieved SL (SL-A) of the design is measured after each step and compared with the SL-T.

The standard [IEC_62443-3-3] also defines a vector format for the joint representation of the three security level types. This format will not be discussed in more detail here. Table 2 shows the definition of the security levels in accordance with [DIN_EN_IEC_62443-3-3]. A more precise definition can be found in Annex 3.2 of the standard.

Table 2: Definition of the security level according to [IEC_62443-3-3] Chapter 3.3

SL	Description
1	Prevent unauthorized disclosure of information by eavesdropping or accidental exposure.
2	Prevent unauthorized disclosure of information to a unit actively seeking it by simple means with low effort, general skills and low motivation.
3	Prevent unauthorized disclosure of information to an entity actively seeking it with sophisticated means and moderate effort, IACS-specific skills and medium motivation.
4	Prevent unauthorized disclosure of information to an entity actively seeking it with sophisticated means and considerable effort, IACS-specific skills and high motivation.

As a rule, operators and planners are faced with the question of which security level is appropriate for a "normal" production facility. There are various publications that deal with this issue. Reference is made here to [EHR2023], [FUH2016] and [ISA2024]. In summary, the authors of the cited publications consider SL2 to be suitable for automation applications without special security requirements.

4. The tasks of the system planner according to IEC 62443

In the IEC 62443 standard, the role of the system planner is also referred to as the integration service provider (service provider) or, more colloquially, the system integrator. The system planner plans the automation system according to the system operator's specifications. The system planner must take the OT security requirements into account in the planning process.

4.1. Relevant parts of the IEC 62443 standard for system planners

The following parts of IEC 62443 are relevant for the work of the system planner as shown in Figure 2:

- **[IEC_62443-2-4]:** This part of the standard deals with requirements for planning and maintenance service providers. The standard includes mastery of the security processes, appropriate qualification and instruction of personnel with regard to OT security requirements, protection of sensitive data, employee screening, provision of tools for OT security, knowledge of hardening automation systems, knowledge of risk assessment, knowledge of network design, etc. This standard is therefore essentially about the required qualification of an engineering service provider / system planner. If an operator carries out system planning in-house, its planning personnel should have the appropriate qualifications.
- **[IEC_62443-3-2]:** This part of IEC 62443 deals, among other things, with risk management and risk assessment of automation systems and specifies the requirements for:
 - "The definition of a system under consideration (SUC, SUC) for an industrial automation system (IACS).
 - The division of the SUC into zones and conduits. A conduit is a logical grouping of communication channels to connect two or more zones with common security requirements.
 - Assessing the risk for each zone and each conduit.
 - The definition of the security level to be achieved (SL-T) for each zone and each conduit.
 - The documentation of the security requirements ."

The system planner will work on these tasks as part of the planning process.

- **[IEC_62443-3-3]:** This part of the standard defines the technical security requirements for the plant to be planned. This part of the standard defines detailed technical system requirements - SR for the automation system based on seven foundational requirements – FR. This includes the definition of the requirements in relation to the security level to be achieved, SL-C by the automation system. The foundational requirements are:
 - Identification and authentication control (IAC)
 - Use control (UC)
 - System integrity (SI)
 - Data confidentiality (DC)
 - Restricted data flow (RDF)
 - Timely response to events (TRE)

- Resource availability (RA)

The system planner defines the system structure based on the requirements of this part of the standard and determines the required security properties of the components used and the required security properties of the environment.

4.2. The tasks of the system planner in detail

The OT security design process from the perspective of a system planner (system integrator) includes the tasks described in the following sub-chapters during the planning phase. These tasks are carried out in coordination with the plant operator, who is usually also the client.

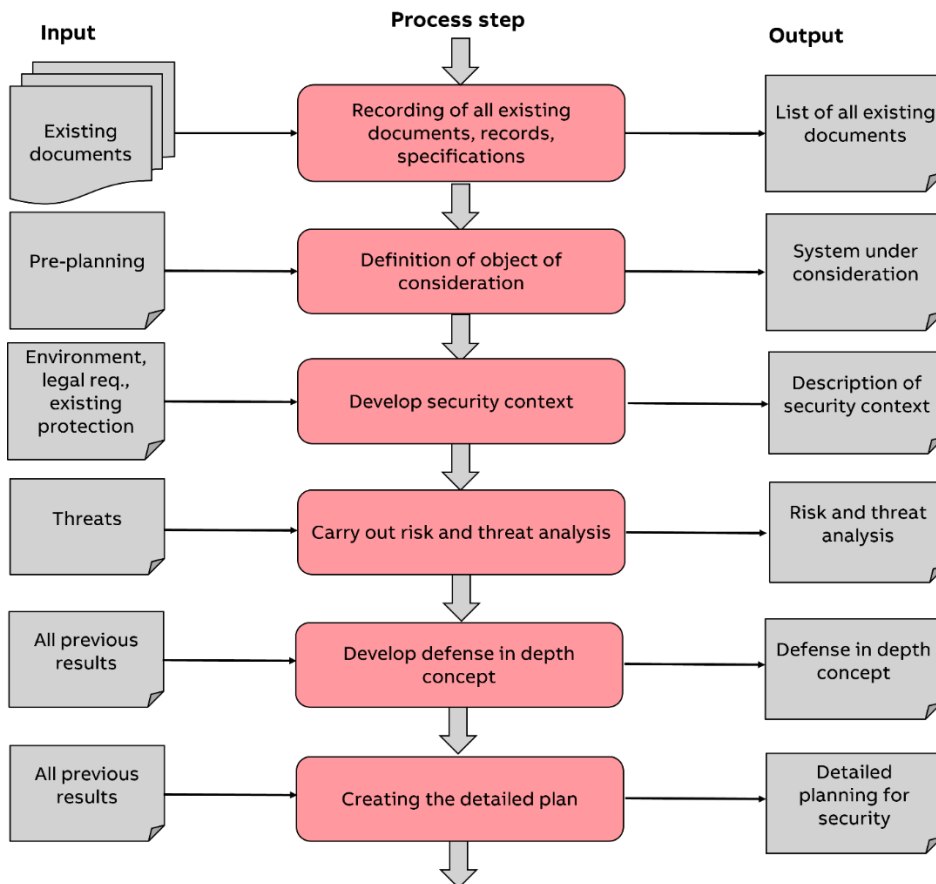


Figure 3: Flow chart for the system planner in the security planning process (image based on [IEC_62443-3-2])

Figure 3 shows the main steps of the security planning process. The individual planning steps are explained in more detail in the following subsections.

4.2.1. Identification of existing documents of the client / system operator

The first step in the planning process is to determine what information the client can provide to the system planner. This involves concepts that have already been developed, descriptions of interfaces to other parts of the system or existing preliminary investigations relating to OT security, e.g. specifications on protection requirements or risk analysis that have already been carried out. The existing information should be recorded and inventoried. It is then available as input for further planning steps.

4.2.2. Definition of the object under consideration (system under consideration)

The basis for the following planning steps is initially the definition of the scope of delivery and the components/system parts that must be considered during the security planning process. The definition ends with a definition of the "System under Consideration" for further security planning. It is important here that system boundaries and interfaces to other systems are defined and documented. The basis for these tasks can be, for example, a tender or preliminary planning by the client, in which the system structure has been fundamentally defined.

4.2.3. Definition of the security context

The security context is defined as follows according to [IEC_62443-1-1]:

"The security context forms the basis for the interpretation of terminology and concepts and shows how the various elements of security relate to each other. The term security is understood here to mean the prevention of illegal or unwanted intrusion into an industrial automation and control system or the disruption of proper and intended operation."

The next step is to define the security context of the system. The security context describes both the risk and the protection factors that are determined by the environment in which the system is operated. This may include location, intended use, operating environment, external protective measures outside the area under consideration and known threats.

Examples of properties of the security context are for example an existing perimeter protection (fence around the factory premises), a video surveillance system or the use of locked control cabinets. However, the security context also includes known threats, such as regular access to the plant, e.g. by visitors or suppliers. Legal and regulatory requirements are also included in the security context.

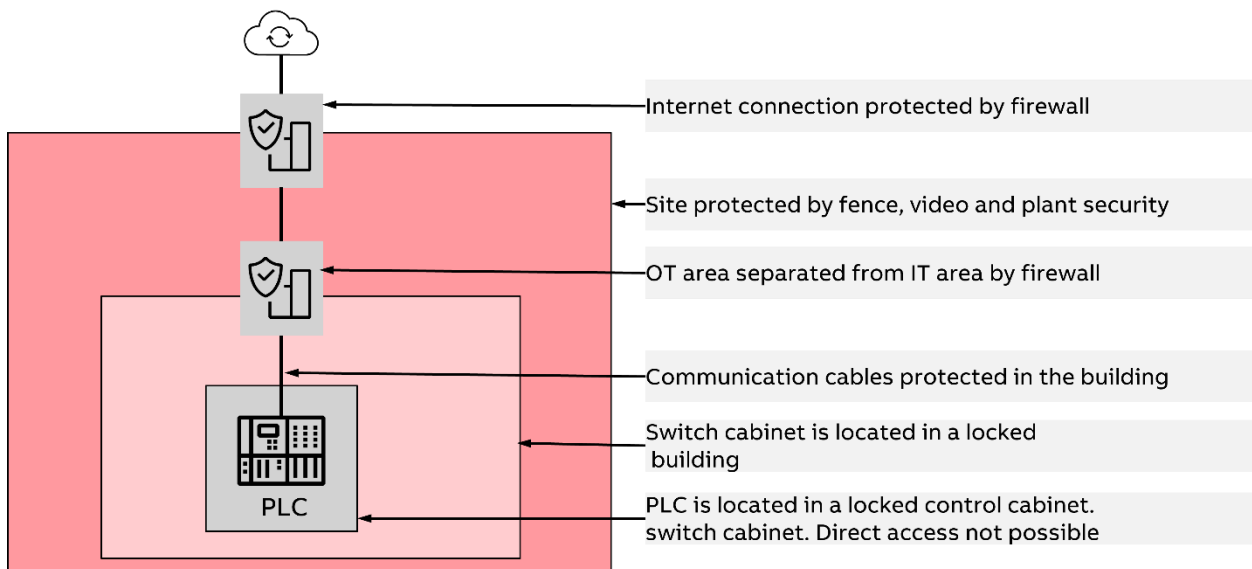


Figure 4: Example of the security context of a PLC

Figure 4 shows an example of the security context of a PLC. The environment in which the PLC is operated already offers a certain degree of protection against possible attacks. For example, a direct attack on the PLC via the control panel or manipulation of the cabling is no longer possible because the PLC is operated in a locked control cabinet. Further protective measures supplement the protection of the PLC. It should be noted that when considering the security context, not only possible protection from the environment, but also possible threats must be considered.

The result of this step is the description of the security context. This is required for the following risk and threat analysis in chapter 4.2.4.

4.2.4. Risk and threat analysis

The [IEC_62443-1-1] says about risk and threat analysis :

" Within the threat-risk assessment process, assets are subject to risks. These risks are in turn minimized through the use of countermeasures, which are applied to address vulnerabilities that are used or exploited by various threats."

The risk and threat analysis is intended to determine which threats an asset is exposed to. The threats are evaluated in terms of the probability of occurrence and the extent of damage and quantified in the form of a risk.

This analysis should identify threats to the automation system or production plant. A risk is defined based on the extent of damage and the probability of damage. If necessary, risk-reducing measures must be defined. Based on the identified risks, the required target security level (SL-T) is defined for the zone under consideration. The procedure for carrying out a risk and threat analysis can be found in [IEC_62443-3-2]. The standard [VDI_2182_1_en] also provides good information on carrying out risk and threat analyses. Suggestions for the tabular documentation of the results can also be found there. Further parts of the standard then describe examples from the manufacturing and process industry for manufacturers, planners and operators.

The risk analysis should be carried out by an interdisciplinary team. Typical roles in this team are according to [VDI_2182_1_en]:

- **“Decision-maker:** Initiator and at the same time decision-maker for the project. The decision-maker determines whether the process is initiated and which of the overall solutions will be implemented in the company. Examples: Managing director, line manager.
- **Security expert:** The security expert acts as a consultant for all security-related IT issues. Their main task is to identify potential threats and threat scenarios for assets, particularly in automation applications, and to suggest possible countermeasures. Examples: OT security consultant, security administrator.
- **System expert:** OT security-relevant questions in an automation system can only be answered in conjunction with technical system knowledge. It is therefore necessary to involve an expert in this field in the process, who acts as a consultant for system-relevant questions. The effectiveness and feasibility of protective measures can only be assessed with his/her help. Examples: System administrator, developer, integrator.
- **Application expert:** In addition to technical system knowledge, knowledge of the entire automation application is also important for the execution of this process. The application expert therefore has an overview of all systems that are relevant for a specific application and knows the overall process and the interrelationships. Examples: Product manager, process engineer.
- **Coordinator:** The coordinator is the active driver of the process. As such, he/she monitors, manages, coordinates and controls the process flow and the players involved. This role is responsible for the overall process and acts as a moderator and leader of meetings that take place within the process. Examples: Project manager, project leader, development manager, line manager.
- **Process auditor:** The process auditor checks all steps of the described process model that have led to the security solution. Examples: external/internal auditor."

The following description assumes that the risk analysis is carried out by the system integrator. However, the system operator's input and personnel must be included in the process.

Structural analysis: A detailed structural analysis should be carried out before the process model is used. This includes a description of the system under consideration and its operating environment. The parameters, functions, interfaces and data flows of the system under consideration should be defined. Application specifics and the network infrastructure should also be described. Visual representation helps to illustrate communication connections and interactions with the operating environment.

Identifying the assets: The next step is to identify the assets. Assets can be, for example: PLCs, operating panels, network components, remote IOs, actuators, sensors, panel PCs, PCs used as operating stations or engineering stations, but also servers. The list of assets can also include intangible assets such as legal positions, intellectual property or others.

Threat analysis: The threat analysis systematically identifies potential organizational, technical and user-related causes of threats. The team must understand the potential vulnerabilities and services of the inspection target. The team can use available threat catalogs such as [BSI2023] (see chapter elementary threats) or [MIT2023] as a basic reference. These catalogs provide typical threat scenarios but should be supplemented by specific application knowledge and expertise of the analysis team. The work should consider the security objectives of the installation. These objectives may be different for different parts of the facility as they may require different levels of protection.

Risk analysis: In this phase, a clear threat matrix should be created that shows which security objectives are affected by the individual threats. This should include both typical threats and their sources, including the actions of authorized and unauthorized users, attackers and malware. This assessment must consider all current countermeasures. The identified risk is analyzed based on the potential damage and the probability of occurrence.

Identification of protective measures: In this step, the necessary countermeasures against threats and their implementation are outlined. Catalogs are used to select suitable measures for all significant risks that need to be mitigated. One or more measures apply to each risk and it must be determined whether single or multiple measures are required. The aim is that the proposed measures reduce the risk sufficiently so that no further mitigation measures are required. Countermeasures should be assessed using the same classes as in the risk analysis (low, medium, high). Often several countermeasures can target the same risk. In addition, the costs associated with a countermeasure, even if it covers multiple threats, should be considered to assess the overall cost-effectiveness.

Selection of protective measures: In this step, countermeasures are selected from a predetermined list that balance cost effectiveness and efficiency. The optimal solution is in line with the company's objectives and security policies. If several cost-comparable counter measures exist, the most suitable one should be selected. Solutions with the same costs may incur different types of expenses, such as depreciation or personnel. The decision should consider cost effectiveness, strategic requirements, feasibility and extension to potential future requirements.

Plan implementation: The selected protective measures must be integrated into the overall planning process of the automation system/production plan.

Process audit: The process audit can be carried out during or after the commissioning phase. See chapter 10.5.

An equivalent analysis in accordance with [IEC_62443-3-2] can be carried out in parallel to the risk analysis described above. The procedure is shown in Figure 5.

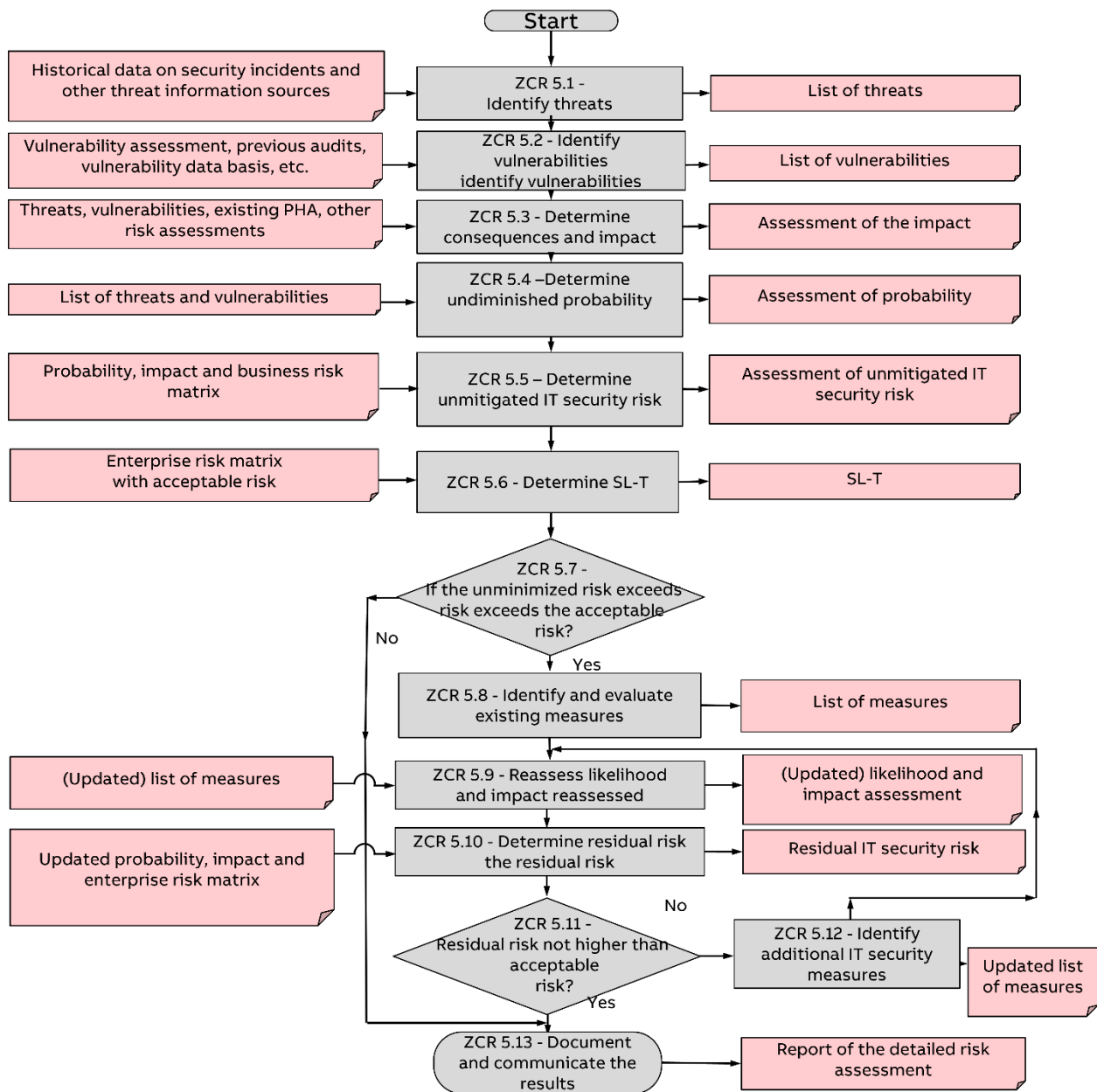


Figure 5: Risk analysis according to [IEC_62443-3-2]

The flow chart for analysis according to this standard is more comprehensive but generally provides the same results. An additional topic covered by the analysis in accordance with [IEC_62443-3-2] is the definition of a target security level (SL-T) in accordance with chapter 3.4, Table 2. It should be noted that the SL-T can be different for different zones of the system. Parts of the system with a higher protection requirement may require a higher SL-T than parts of the system with a lower protection requirement. In addition, the SL-T can be defined differently for individual requirements if necessary. This is the case, for example, if individual requirements are of particular importance for certain parts of the system.

4.2.5. Defense in Depth Concept

The Defense In-Depth approach [DHS2016] is based on the use of multiple layers of security to prevent the failure of a single security component. By combining the various measures at different levels of the system, the level of protection is increased for the entire system by creating appropriate zones. Figure 6 shows an example of the logical and physical trust boundaries for an automation system.

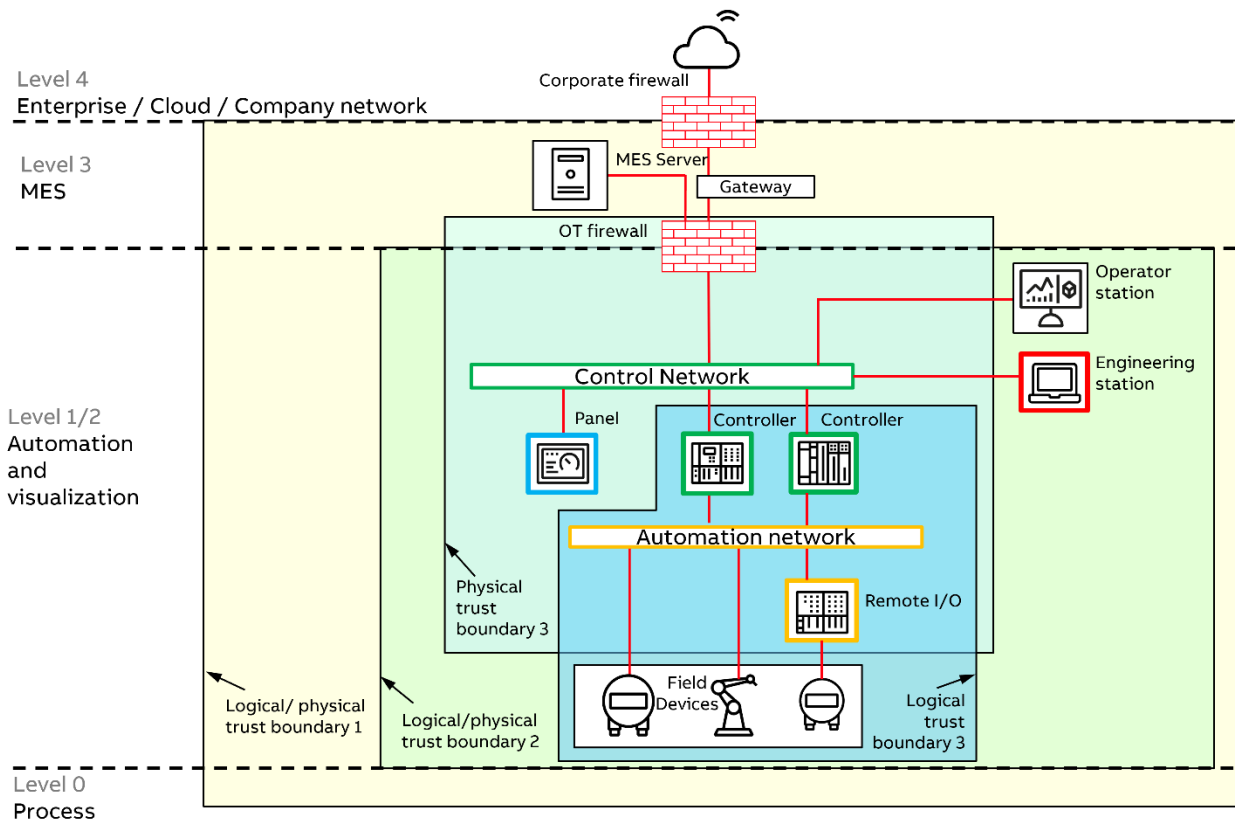


Figure 6: Trust boundaries and zoning in an automation system

In Figure 6 one of the zones is shown in yellow. This zone is framed by the logical/physical trust boundary 1. The physical trust boundary is formed, for example, by a fence around the factory premises in conjunction with a monitoring system and an access-monitored premises. The logical trust boundary 1 is formed by the company firewall. The logical/physical trust boundary 2 frames the zone marked in green. This can be formed, for example, by a production building with access monitoring. Logical trust boundary 2 forms the OT firewall. The physical trust boundary 3 could, for example, be formed by a locked switch cabinet or a locked control room within the production building, which protects the automation components against physical access. Logical trust boundary 3 is formed, for example, by cryptographically secured communication within the automation network, e.g. PROFINET communication in conjunction with PROFINET security [PNO2019]. Figure 6 shows how the various protective measures complement each other as part of the defense-in-depth concept.

As part of planning in accordance with [IEC_62443-3-3], the defense-in-depth concept is supplemented by the zone and conduit concept. The following steps are recommended for implementing the zone-and-conduit concept:

1. Plan the network and define the zones and conduits: Security is based on the separation of networks (e.g. by firewalls) to protect the automation network from external threats. The separated parts of the network are called zones. A conduit is a logical grouping of communication channels to connect two or more zones that have common security requirements.
2. Plan general security features for the automation system / production plant based on the risk and threat analysis.
3. Document the results of the planning process.
4. Obtain approval / sign-off from the customer / plant operator.

Further tasks for the system integrator, such as safe commissioning and system hardening, follow in later chapters of this document (see chapter 4.3).

4.2.6. Creating the detailed planning

Based on the preliminary work, a detailed plan is then created which implements the security requirements of [IEC_62443-3-3]. This includes, for example, specifying which communication protocols are to be used in which form and which automation components with which properties are to be used.

Furthermore, as part of the detailed planning, a plan should also be drawn up for the hardening of the system during commissioning and the information required for this should be obtained. Hardening means switching off services and functions that are not required and selecting configuration settings that are as secure as possible, e.g. for the operating system of PCs. There are several documents on hardening automation systems, some of which are mentioned here: [BSI2021b], [BSI2021a], [NAM2017], [NIST_SP_800-82], [PUL2025], [ZOR2025].

4.2.7. Results of the planning process

The planning work described in the previous steps leads to the following results:

- List of all existing documents
- Description of the system under consideration
- Description of the security context
- Risk and threat analysis
- Defense in depth concept with zoning and target security level SL-T
- Detailed security planning

The results should be documented and archived for later use. In the event of significant changes or after a certain period, risk and threat analysis should be updated.

4.3. Interaction of the planner with the other responsible parties in the OT security process

Figure 7 shows the interaction between the operator, planner and manufacturer in the OT security process.

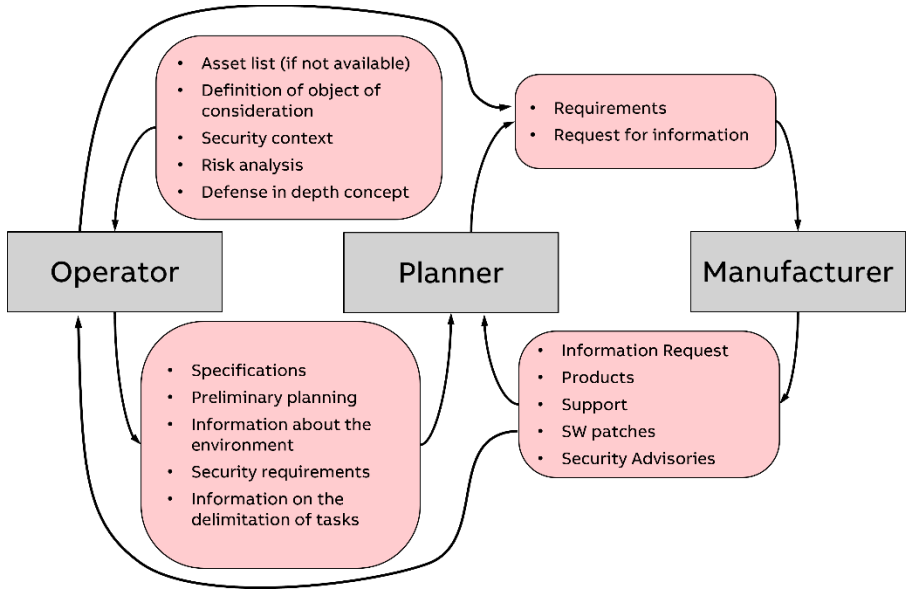


Figure 7: Interaction between planner, operator and manufacturer

The operator, who is usually also the client for the planner, provides the planner with existing preliminary plans and considerations and makes specifications for the planning process. At the same time, he provides information about the operating environment, as the planner needs to know this for risk assessment. Furthermore, the planner must define which tasks he himself and which tasks the planner should take on in the security process. Both the operator and the planner are in contact with the manufacturer who will supply the automation system or essential parts of it. Essentially, the manufacturer is asked to fulfill security requirements and provide technical information, which is then supplied to the operator and/or planner. In addition, the manufacturer provides security advisories and the associated software patches when vulnerabilities occur.

4.4. Proposal for the realization of the security requirements

It is proposed to carry out the planning process as shown in Figure 3. The main steps described there are broken down into work packages as shown in Table 3.

Table 3: Work packages for the security planning process

Step	Task	Responsible
B1	Definition of the tasks for the planner, delimitation of the tasks of the operator and planner, commissioning of the planner to the agreed extent.	Operator
B2	Recording and inventory of all necessary documents and forwarding to the planner.	Operator
B3	Documentation of the handover	Operator, confirmation planner.

P4	Definition of object under consideration, description of interfaces	Planner, confirmation operator
P5	Description of security context, if this is not yet available, based on the information provided by the operator.	Planner, confirmation by operator
P6	Carry out a risk and threat analysis	Planner, confirmation by the operator that the residual risks have been noted and are accepted.
P7	Develop a defense in depth and the zone and conduit concept	Planner, acceptance by operator
P9	Preparation of the detailed planning	Planner, acceptance by operator.
P10	Planning the hardening of the system	Planner, acceptance of the procedure by the operator
P11	Documentation and results. This particularly involves the creation and provision of asset lists, network structure plans and the configuration of firewalls, for example.	Planner, acceptance and check for completeness by the operator.

It should be noted that the work plan described in Table 3 is merely a basic framework that must be adapted to the circumstances of the respective project.

4.5. Success factors for the OT security process of system planners

There are several prerequisites that must be met for a successful and efficient planning process. The main ones are:

- Clear description of the subject of the order.
- Description of all security-relevant activities in a task description/requirement specification and commissioning of these services.
- Early and complete provision of all preliminary work / preliminary considerations by the client.
- Clear delineation of responsibilities between operator and planner.
- Confirmation of the work packages listed in Table 3.
- Security briefing of the commissioning personnel.
- Provision of a PC (preferably in a demilitarized zone) to receive the system project planning from the system planner.

5. The tasks of the system operator according to IEC 62443

This chapter deals with the tasks of the system operator. In addition to the tasks already described in Table 3. Regarding the provision of information and acceptance of work results, the operator must perform specific tasks during the operating phase and when decommissioning the system.

5.1. Relevant parts of the IEC 62443 standard for system operators

The following parts of IEC 62443 are relevant to the work of the system operator as shown in Figure 2:

[IEC_62443-2-1] describes the processes that a plant operator must establish and maintain to ensure the safe operation of the plant. The personnel responsible for operating the system are also included in this consideration. The standard defines requirements for the establishment, implementation, maintenance and continuous improvement of an IACS security program. The purpose of the security program is to reduce IACS security risks to an acceptable level. These requirements in the standard are written to be independent of implementation so that operators can choose the approaches best suited to their needs. The document uses a risk-based approach; the requirements are designed to reduce existing security operational risks to an acceptable level. Essential requirements of the standard are e.g.:

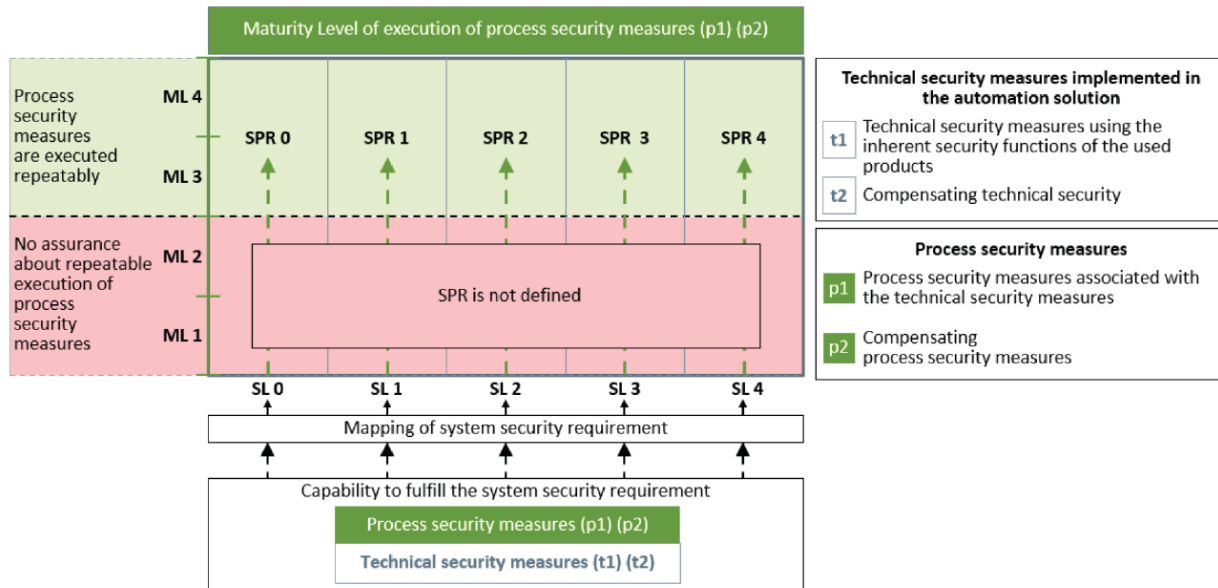
- Qualification of personnel.
- Training of employees, contractors, subcontractors, consultants and suppliers with regard to OT security.
- Security of the supply chain: Definition of requirements for service providers and suppliers.
- Identification and reduction of IT security risks.
- Establishment of processes to detect IT security anomalies.
- Use of components that have been developed in accordance with the secure development life cycle (see [IEC_62443-4-1]).
- Regular verification and adaptation of the security program.
- Limitation and control of access to the automation system.
- Inventory of hardware and software components.
- Creation and maintenance of the system documentation (e.g. asset lists and network plans).
- Documenting the configuration information for all components and updating the documentation accordingly.
- Defining the network segmentation and monitoring its maintenance.
- Planning the system in such a way that it can continue to work (possibly with restrictions) even if it is disconnected from the rest of the network.
- Identification and authentication of devices that are connected to the network.

This list is only an excerpt from the standard. Other points are, for example, wireless networks, secure remote access, component security (protection of interfaces), hardening of devices, mobile data carriers, protection against malware, patch management (there is also a separate standard section [IEC_TR_62443-2-3], predefined system states in the event of a fault, etc..

It has already been pointed out in the chapter 3.1 that the OT security program can also be combined with any existing security program in the company in accordance with ISO 27000. Details on this can be found in [NIE2021], [NIE2024].

[IEC_62443-2-2] deals with a methodology for evaluating the protection of industrial automation systems. Here, organizational and technical measures are considered in parallel and evaluated in an overall value, the so-called "Security Program Rating " (SPR). The methodology is based on the fulfilment of technical and organizational requirements that are defined in the relevant documents of the IEC 62443 series of standards.

The aim of this approach is to show that the security properties of a production facility are described not only by the technical requirements, but also by the maturity level of the organization.



IEC

Figure 8: Security Program Rating according to [IEC_62443-2-2]

Figure 8 shows an excerpt from [IEC_62443-2-2]. The possible security levels SL1 to SL4 are plotted on the abscissa. These define the technical security properties of the implemented automation system (SL1 is the lowest value, SL4 the highest). The maturity levels ML1 to ML4 are shown on the ordinate. These describe the maturity level of the system operator's organization (ML1 is the lowest level, ML4 the highest). After selecting a Security Level SL and a Maturity Level ML, the corresponding Security Program Rating (SPR) can be read from the matrix. Both a high SL and a high ML are required for a high SPR. This reinforces the statement that security can only be realized through a combination of technology and processes.

The standard section [IEC_TR_62443-2-3] looks at patch management for automation systems. It deals with the interaction between the manufacturer and operator regarding security patches. The standard defines a status model for manufacturers and operators about the test and release status of patches. It also defines a data format for the standardized and machine-readable exchange of information.

[IEC_62443-2-4]: This part of the standard deals with requirements and planning and maintenance service providers and has already been described in chapter 4.1 .

The [IEC_62443-2-5] part is intended to provide implementation instructions. This part has not yet been published.

5.2. The tasks of the system operator in detail

Figure 9 provides an overview of the tasks of the system operator in the security process. A distinction is made here between tasks that arise for a specific installation and continuous tasks that arise for the entire site.

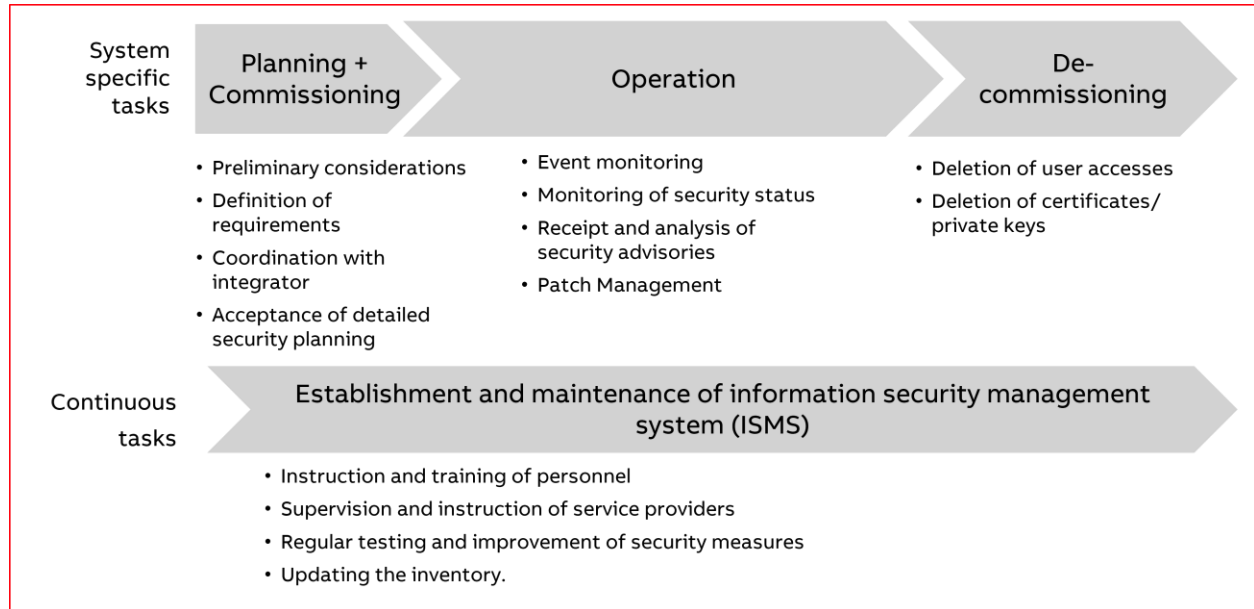


Figure 9: Tasks of the system operator

The system-specific tasks in **the planning and commissioning phase** were described in chapter 4.3. Please refer to Table 3.

The **operating phase** begins with the handover of the system from the planner to the operator. It is assumed that all necessary technical security precautions have been planned and put into operation. In this case, the operator has the following tasks, for example:

- Monitoring the security events that occur and triggering an appropriate response. This can be done, for example, as part of a Security Information and Event Management System (SIEM).
- Maintaining the system documentation in the event of changes, e.g. asset lists, network plans.
- Monitoring the security status of the system and reacting to events, e.g. through automated evaluation of log information.
- Receipt and evaluation of security advisories from the control system manufacturer. Checking whether hardware or software updates should be applied to the installed assets based on these advisories. Carrying out a risk assessment regarding the installation time and, if necessary, defining risk-minimizing alternative measures if patches cannot be installed promptly.
- Test the software updates regarding use in your own system. Planning of hardware and/or software updates.
- Updating the risk and threat analysis at regular intervals, in the event of changes to the system or known incidents.

During the **decommissioning phase**, the user access credentials used in the system must essentially be deleted so that access to the components is no longer possible. Hard disks of servers and computers should be deleted before scraping and the data carriers overwritten with random patterns. Any stored certificates or private keys of the operator should be deleted before scraping. If this is not possible, the module should be destroyed.

In addition to these system-specific activities, the operator must also set up and operate an information security management system (ISMS). This is a general and not a system-specific task. Reference is made here to [IEC_62443-2-1], in which the necessary activities are documented in the form of requirements. An excerpt of the required activities was described in chapter 5.1.

5.3. Cooperation with the other responsible parties in the OT security process

The interaction of the operator with the other responsible parties in the OT security process has already been explained in chapter 4.3. Reference is made here to Figure 7 and the associated explanations.

5.4. Proposal for a procedure for implementing the requirements for operators

It is proposed to proceed in accordance with the breakdown in Figure 9 and to manage the plant-specific parts and the continuous tasks in separate work packages. If a plant consists of several systems, synergy effects can be used here. In any case, the appointment of an OT security officer is recommended. Table 4 provides an overview of possible work packages. A distinction is made here between the continuous, central tasks “Cx” and the system-specific tasks “Sx”. Table 4 lists basic activities that must be adapted to the requirements of the respective operator.

Table 4: Work packages for the security process for operators

Step	Task	Responsible
C1	Set up an ISMS , preferably in coordination with the IT department. If already in place: Link to an existing company ISMS.	OT security officer
C2	Training of employees: Training of employees, contractors, subcontractors, consultants and suppliers with regard to OT security.	Person responsible for OT security
C3	Security of the supply chain : Definition of general requirements for service providers and suppliers that are not project-specific (applicable OT security documents).	Person responsible for OT security
C4	Establishment of processes for detecting IT security anomalies e.g. through the central evaluation of log data . Provision of such a system and connection of the automation systems.	OT security officer
C5	Creation of an OT security policy. Instruction of employees and service providers. Compliance monitoring.	OT security officer
C6	Creating a standardized company concept for remote maintenance of the systems. Clarification of the requirements with the system managers. Standardized implementation for as many systems as possible.	OT security officer
S7	Creation of an emergency and restart plan for the company. Roll out the plan. Carry out emergency drills.	OT security officer
S8	For systems that fall under the NIS2 directive: Create a reporting system for reporting security-relevant incidents.	OT security officer
S9	Creation and implementation of a central backup concept for OT. Rolling out the concept and carrying out restore exercises.	OT security officer

S10	Supporting the planner in planning and commissioning regarding security aspects	Person responsible for OT security
S11	Monitoring compliance with the security guidelines for the plant.	Person responsible for OT security
S12	Responding to security events that are detected during monitoring. For systems in the critical infrastructure (KRITIS) or for systems that fall under the NIS2 directive: Submit a report via the company's defined channel.	Person responsible for OT security
S13	Monitoring the security advisories of the control system and component manufacturers and deriving measures for the system.	OT security officer
S14	Receipt of software patches from system or component manufacturers. Checking the patches for suitability and relevance. If necessary, planning and implementation of software updates	OT security officer
S15	Updating the risk and threat analysis at regular intervals, in the event of changes to the system or known incidents	Person responsible for OT security

5.5. Success factors for the security process of plant operators

There are a number of prerequisites that must be met for the successful and efficient operation of production facilities. The main ones are:

- Management commitment to the need for IT and OT security in the company.
- Appointment of an OT security officer.
- Integration of the OT security officer(s) into the company's security process.
- Close exchange between those responsible for IT and OT security.
- Creation of an OT security guideline for the operation of production facilities.
- Integration of OT security requirements into the supply chain (manufacturers and system integrators).
- Automated asset management.
- Require suppliers to provide machine-readable security advisories.
- Security training of personnel and service providers.
- Continuous monitoring and improvement of security processes according to a plan, do, check, act approach.

The above list is only an excerpt of possible success factors.

6. Summary

According to [IEC_62443-1-1], security is based on the components shown in Figure 10 .

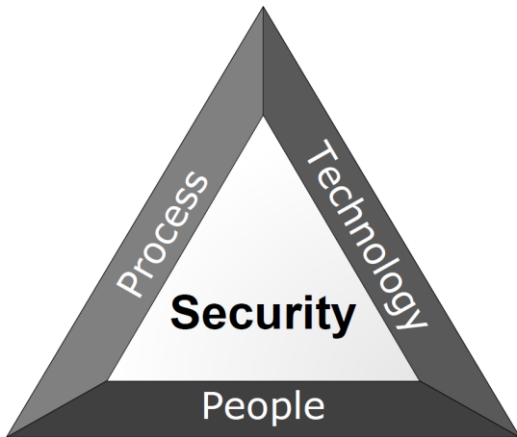


Figure 10: The components of security [IEC_62443-1-1]

The message of Figure 10 is that OT security is not only achieved through **technical measures** such as firewalls or network monitoring, but also through the associated **processes**. Network monitoring is only useful to the company if the events that occur are evaluated and responded to appropriately and promptly. This is only possible through the associated processes, which must be established and operated in a stable manner. It should be noted that the security processes follow a risk-based approach. The aim is to reduce risk to an acceptable level, which results in an acceptable compromise between security, costs, operability and system availability, among other things. **People** are the third component in achieving good OT security. A stable security process can only be achieved through regular training (emergency drills, backup and restore exercises) and the specification of clear guidelines (what am I allowed to do, what am I not allowed to do).

7. List of figures

Figure 1: Overview of the IEC 62443 series of standards, based on [DKE2024]	7
Figure 2: Stakeholders in the OT security process and assigned parts of IEC 62443 (derived from [IEC_62443-4-1])	9
Figure 3: Flow chart for the system planner in the security planning process (image based on [IEC_62443-3-2])	13
Figure 4: Example of the security context of a PLC	14
Figure 5: Risk analysis according to [IEC_62443-3-2]	17
Figure 6: Trust boundaries and zoning in an automation system.....	18
Figure 7: Interaction between planner, operator and manufacturer	20
Figure 8: Security Program Rating according to [IEC_62443-2-2]	23
Figure 9: Tasks of the system operator	24
Figure 10: The components of security [IEC_62443-1-1].....	27



8. List of tables

Table 1: Differentiation between IT and OT according to [GAR2021]	6
Table 2: Definition of the security level according to [IEC_62443-3-3] Chapter 3.3.....	11
Table 3: Work packages for the security planning process.....	20
Table 4: Work packages for the security process for operators	25

9. Index

Access limitation	22	Maintenance service providers	23
Achieved SL.....	10	Monitoring	26
Anomalies	25	Network segmentation.....	22
Application expert.....	15	NIS2.....	5, 25
Asset identification	16	Non-repudiation	6
Asset management.....	26	Operating environment	14
Asset owner	5	Operating phase.....	24
Authentication	12, 22	Operational Technology	6
Authenticity	6	Operators.....	7
Automation components	8	OT.....	6
Automation system	20	OT security guideline.....	26
Availability.....	6	OT security officer	25, 26
Backup	25	OT security policy.....	25
Capability SL.....	10	Patch management.....	23
Commitment.....	26	Patch Management.....	6
Conduits.....	12	Perimeter protection.....	14
Confidentiality	6, 12	Plant operator	9
Configuration information	22	Principles.....	7
Coordinator	15	Probability of occurrence	16
Damage	16	Process audit.....	16
DC	12	Process auditor.....	15
Decision maker	15	Product supplier	8, 9
Decommissioning	24	Protection requirements	13
Defense in depth.....	5, 17, 19	Protective measures.....	16
Detailed planning	19	Qualification.....	22
Elementary threats	16	RA	13
Emergency and restart plan	25	RDF	12
Evaluation	8	Reaction to events	24
Events	12	Remote access	22
Foundational requirements	12	Remote maintenance	25
FR	12	Requirement specification.....	21
Hardening	19, 21	Requirements automation systems	8
IAC.....	12	Resource availability	13
IACS	7	Responsibilities	21
IACS-security program.....	22	Restricted data flow	12
Identification.....	12	Risk analysis	13, 16
IEC 62443	5, 7	Risk and threat analysis.....	15
Overview.....	7	Roles OT security process	8
Information Security Management System .	5, 25	Secure development lifecycle	22
Information technology.....	6	Security advisories.....	24
Information Technology.....	6	Security context.....	14, 19
Integration service provider	12	Security detail planning	19
Integrity.....	6	Security events	24
Inventory	22	Security expert.....	15
ISMS.....	5, 6, 25	Security guidelines.....	26
ISO 27000.....	8, 23	Security level.....	10, 11, 12
IT 6		Security process	12
IT security risks.....	22	Security Program Rating	23
KRITIS.....	26	Security requirements.....	12
Log information	25	Security status	24

Security training 26
 Separation22
 Service provider8, 12
 SI12
 SL-A10
 SL-C10, 12
 SL-T.....10, 12, 15
 SPR.....23
 SR12
 Structural analysis16
 SUC12
 Success factors21, 26
 Supply chain 22, 25
 System documentation 22, 24
 System expert15
 System integrator 8, 9, 12
 System integrity12

System operator..... 8, 22
 System planner12
 System planner tasks13
 System requirements12
 System supplier 8
 System under consideration12, 14
 Target SL 10
 Terms7
 Threat analysis16
 Training 22, 25
 TRE12
 Trust boundary18
 UC.....12
 Use control.....12
 Wireless networks22
 Zones..... 12, 17

10. Bibliography

- [BSI2021a] Bundesamt für Sicherheit in der Informationstechnik (BSI): IND.1: Prozessleit- und Automatisierungstechnik. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium Einzel PDFs 2021/08 IND Industrielle IT/IND_1_Prozessleit_und_Automatisierungstechnik_Edition_2021.pdf?__blob=publicationFile&v=2.
- [BSI2021b] Bundesamt für Sicherheit in der Informationstechnik (BSI): Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln. URL: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen zur Haertung von Windows_10.pdf?__blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen_zur_Haertung_von_Windows_10.pdf?__blob=publicationFile&v=3).
- [BSI2023] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompodium. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4#download=1.
- [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_ICSCERT_Defense_in_Depth_2016_S508C.pdf.
- [DKE2024] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE: IEC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung. URL: <https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung>.
- [EHR2023] Ehrlich, Marco; Bröring, Andre; Diedrich, Christian; Jasperneite, Jürgen; Kastner, Wolfgang; Trsek, Henning: Determining the Target Security Level for Automated Security Risk Assessments: 2023 IEEE 21st International Conference on Industrial Informatics (INDIN). IEEE, 2023 - 2023; S. 1–6.
- [FUH2016] Fuhr, David et al.: Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau. URL: <https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/vdma-security-automation.html>.
- [GAR2021] Gartner Inc.: Gartner Glossary Information Technology. URL: <https://www.gartner.com/en/information-technology/glossary>.
- [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_62443-2-1] 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_62443-2-5] IEC- International Electrotechnical Commission, IEC 62443-2-5: Implementation guidance for IACS asset owners, not released.
- [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_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>.
- [ISA2024] ISA - The International Society of Automation: The Case for ISA/IEC 62443 Security Level 2 as a Minimum for COTS Components. URL: <https://www.isasecure.org/hubfs/The-Case-for-ISA-IEC-62443-Security-Level-2-as-a-Minimum-FINAL.pdf>.
- [ISA2025] ISA - The International Society of Automation: ISA/IEC 62443 Series of Standards. URL: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.
- [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>.
- [MIT2023] Mitre Corporation: MITRE ATT&C ICS Matrix. URL: <https://attack.mitre.org/matrices/ics/>.
- [NAM2017] NAMUR AK 4.18 Automation Security: Härtung von Computersystemen. URL: https://www.namur.net/fileadmin/media_www/Dokumente/AK-PRAXIS_4.18_Haertung_2017-09-11.pdf.
- [NIE2021] Niemann, Karl-Heinz: Differentiation of the IT security standard series ISO 27000 and IEC 62443. Whitepaper. URL: https://library.e.abb.com/public/fc76636ebed845b88c640a613f0c95a0/3ADR010839_Differentiation_ISO_27001_IEC_62443_REV_C_en_US.pdf.
- [NIE2024] 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>.
- [NIS2_en]: Directive (EU) 2022/2555 of the European Parliament 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.

- [NIST_SP_800-82] National Institute of Standards and Technology (NIST), SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security, 2023. URL: <https://nvl-pubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>.
- [PNO2019] PROFIBUS Nutzerorganisation e. V.: Security Extensions for PROFINET. PI White Paper for PROFINET. URL: <https://www.profinet.com/download/pi-white-paper-security-extensions-for-profinet/>.
- [PUL2025] Puls, Jan-Niklas; Niemann, Karl-Heinz: Härtung in der industriellen IT: Schutzmaßnahme gegen Cyberangriffe. In Zukunft.Digital - Zeitschrift des Mittelstand Digitalzentrums Hannover, Ausgabe 01/2025, 2025; S. 20–22. URL: https://digitalzentrum-hannover.de/wp-content/uploads/2025/06/MDZH_Magazin_25-01_web_25-06-16.pdf.
- [TRE2022] Trend Micro Inc.: The State of Industrial Cybersecurity. 2022 industrial cybersecurity survey report in manufacturing, electric utilities, oil, and gas. URL: https://www.trendmicro.com/en_us/research/22/f/state-of-ot-security-2022.html.
- [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>.
- [ZOR2025] Zorlu, Nurullah: Bestandsaufnahme zur Härtung von Automatisierungssystemen im Sinne der OT-Security. Bachelor Thesis. URL: <https://doi.org/10.25968/opus-3581>.

ABB LTD.

Contact:

<https://access.motion.abb.com/contact/contact>

Homepage:

www.abb.com/plc

—

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents - in whole or in part - is forbidden without prior written consent of ABB AG.
Copyright© 2025 ABB. All rights reserved.