WHITEPAPER

Differentiation of the IT security standard series ISO 27000 and IEC 62443

A view of automation systems in the manufacturing and process industries

"Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443"
https://doi.org/10.25968/opus-1973

NOTE: This is a courtesy translation only. In case of discrepancy between the German language original text and the English language translation, the German version shall prevail. This includes any extracts from standards as they have been taken from the German standard versions, not from the official English equivalents.

This white paper was created in cooperation with **ABB AG**, Heidelberg, Germany.

Photos: Adobe Stock / Fotolia

Table of contents

1. Introduction

Planners and operators of production facilities are faced with the question of which standards are to be adhered to for the IT security concepts and, if necessary, also for auditing these facilities. Since the responsibility for IT security for operational technology (OT) often lies in different hands than for information technology (IT), there are occasionally divergent views as to which standards are to be used as a basis.

People from the IT environment usually focus on the ISO 27001 series of standards, while people from the OT environment tend to prefer the IEC 62443 series of standards. This article describes the basics and focus of the two series of standards and makes suggestions as to when it makes sense to adhere to one standard in particular, or to both standards jointly.

The document closes with a recommendation for a procedure with regard to production systems for the manufacturing and process industries (OT security). Finally, in the appendix, the applicability of the standards is discussed using the example of a wastewater treatment plant.

2. Overview of IT security norms and standards

In the area of IT security, companies have access to a number of standards or series of standards, as well as recommendations from manufacturers' associations and authorities. The standards define the state of the art and thus enable a standardized procedure regarding the design, implementation, operation, and certification of IT security systems.

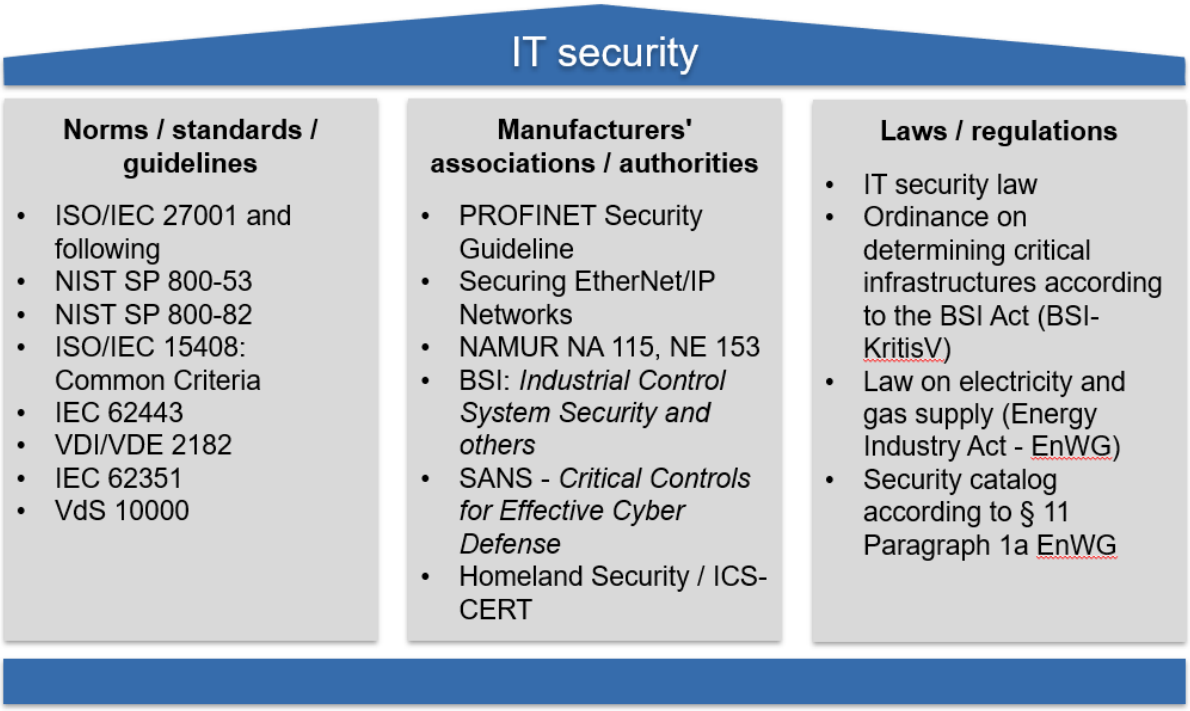

Figure 1: Overview of norms and standards for IT security

Figure 1 gives an overview of norms and standards for IT security. In addition to general standards (ISO 27000 series, IEC 15408, German Federal Office for Information Security (BSI) IT baseline protection "Grundschutzkatalog"), standards are also listed that specifically address the production area (IEC 62443, IEC 62351, VDI/VDE 2182). The list is supplemented by a number of standards from manufacturer / user associations (PROFINET, EtherNet/IP, NAMUR) and authorities (BSI, Homeland Security).

The following sections mainly focus on the ISO 27000 and IEC 62443 series of standards. It should be noted that both series of standards are still being developed. The standardization roadmap IT security of the German Electrotechnical Commission [DKE2017] provides an overview of current and future work. A description of the other norms and standards mentioned in Figure 1can be found in [NIE2017].

2.1. The ISO 27000 series of standards

The ISO 27000 series of standards is a series of sixty sub-standards on the subject of information security management systems, hereinafter referred to as ISMS. An introduction and overview of the individual sub-standards including a short description can be found in [DIN_EN_ISO_27000] or online at [ISE2020]. The following sections describe the essential

parts of the series of standards.

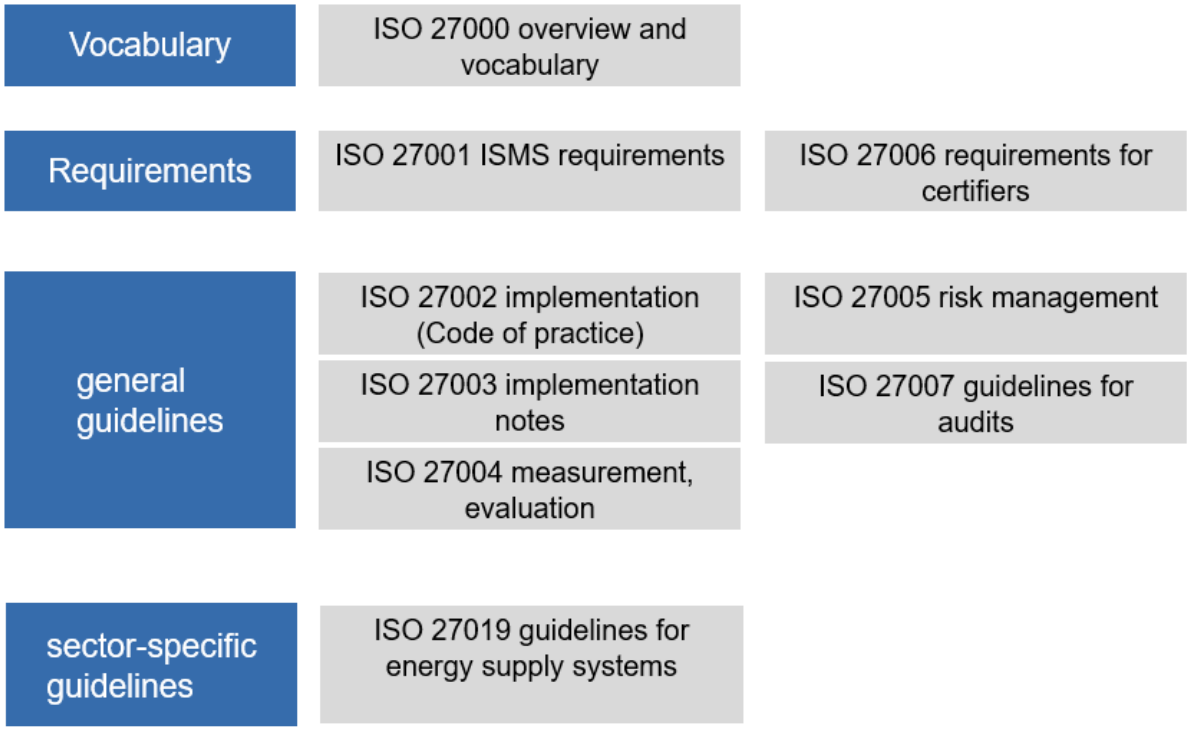

Figure 2: Extract from the structure of the ISO 27000 series of standards based on [KRO2017]

Figure 2 gives an overview of the essential parts of the ISO 27000 series of standards. The series of standards is divided into four main parts: Vocabulary and overview, requirements, general guidelines, and sector-specific guidelines. The standard parts mentioned in Figure 2 constitute an excerpt listing only the most important parts of the series of standards.

2.1.1. Vocabulary and overview

The **[DIN_EN_ISO_27000]** first explains the technical terms used and then gives an overview of the other standards included in the series of standards. The series of standards deals with the structure of an information security management system (ISMS). This is defined according to [DIN_EN_ISO_27000] as follows:

> *"An information security management system (ISMS) includes policies, procedures, guidelines, and related resources and activities, all of which are controlled by an organization to protect its information assets. An ISMS is a systematic model for introducing, implementing, operating, monitoring, reviewing, maintaining, and improving the information security of an organization in order to achieve business goals. It is based on a risk assessment and the risk acceptance level of the organization and is used to treat and manage the risks effectively. A requirements analysis for the protection of information assets and the implementation of appropriate measures to ensure the protection of these information assets as required contributes to the successful implementation of an ISMS."*

The standard focuses on information security in order to ensure the confidentiality, availability, and integrity of information. It takes a process-oriented approach in order to identify and control the necessary processes in the company. The series of standards follows a risk-based

approach in which information security risks are described, assessed, and dealt with. The maintenance and improvement of the ISMS are monitored, controlled, and continuously enhanced in a continuous improvement process.

2.1.2. Requirements

[DIN_EN_ISO_27001] defines requirements for ISMSs. It defines the requirements for the introduction, implementation, operation, monitoring, review, maintenance, and improvement of formalized information security management systems (ISMS) in connection with the overarching business risks of an organization. The content includes:

- Context of the organization
- Management leadership and commitment
- Company security policy
- An organization's roles, responsibilities, and authorities
- Measures for dealing with risks and opportunities
- Support, communication, documentation
- Operation
- Evaluation of performance
- Improvement process

[ISO_27006] specifies requirements and offers instructions for bodies that carry out audits and certifications of an information security management system (ISMS). It is primarily intended to support the accreditation of certification bodies that offer ISMS certifications.

Expert knowledge about the requirements and reliability has to be proven by every entity offering ISMS certification, and the guideline contained in this International Standard provides an additional interpretation of these requirements for any entity offering ISMS certification. This standard can be used as a catalog of criteria for audits.

2.1.3. General guidelines

The part of the general guidelines for the ISO 27000 series consists of several standards, which are briefly described below.

[DIN_EN_ISO_IEC_27002] is a guide for the implementation of information security measures. In particular, Sections 5 to 18 give specific advice and guidance on best practices for implementing the measures set out in [DIN_EN_ISO_27001], A.5 to A.18. These include, for example:

- Allocation of access rights, user administration, access administration, password management.
- Disposal of data carriers
- Access to networks and network services
- Key management
- Physical security perimeter
- Securing rooms and facilities
- Operational processes and responsibilities
- Protection against malware
- Data back-up

- Network security management, network segregation
- Supplier relationships
- and much more

The above list is not a complete excerpt from the standard, it is only intended to serve as an exemplary list.

[ISO_27003] provides guidelines on the requirements for an information security management system (ISMS), as specified in ISO/IEC 27001, and gives recommendations in relation to these. Sections 4 to 10 of this document reflect the structure of [DIN_EN_ISO_27001]. [ISO_27003] does not define any new requirements but provides explanations and implementation recommendations for a better understanding. There is therefore no obligation to follow the instructions in this document.

[ISO_27004] provides guidance to support organizations in evaluating the information security performance and effectiveness of an ISMS in order to meet the requirements of ISO/IEC [DIN_EN_ISO_27001] Section 9.1. It addresses:

- the monitoring and measurement of information security performance;
- the monitoring and measurement of the effectiveness of an information security management system including its processes and measures;
- the analysis and evaluation of the monitoring and measurement results.

[ISO_27004] thus provides a framework that makes it possible to measure and evaluate the effectiveness of ISMS in accordance with [DIN_EN_ISO_27001]. It furthermore includes a description of security indicators and how to obtain them.

The **[ISO_27005]** contains guidelines for the risk management of information security. It supports the general concepts specified in [DIN_EN_ISO_27001] and is intended to support the implementation of information security on the basis of a risk management approach. Knowledge of the concepts, models, processes, and terminology described in [DIN_EN_ISO_27001] and [DIN_EN_ISO_IEC_27002] is important for a complete understanding. This document is applicable to all types of organizations (e.g. business enterprises, government agencies, non-profit organizations) intending to manage risks that may endanger the organization's information security.

[ISO_27007] provides guidance for organizations which carry out internal or external audits of an ISMS or which have to handle an ISMS audit program in accordance with the requirements specified in ISO/IEC 27001.

An information security management system (ISMS) audit can be performed using a number of audit criteria, such as:

- Requirements defined in [DIN_EN_ISO_27001];
- Guidelines and requirements established by relevant interested parties;
- legal and regulatory requirements;
- ISMS processes and controls defined by the organization or other parties;
- Management system plan(s) that relate to the provision of specific results of an ISMS (e.g. plans for dealing with risks and opportunities when establishing the ISMS, plans for achieving information security targets, risk management plans, project plans).

The standard provides guidance for all sizes and types of organizations and ISMS audits of various sizes. The document focuses on internal ISMS audits (first party) and ISMS audits which are carried out by organizations at their external service providers (second party).

2.1.4. Sector-specific guidelines

The ISO-27000 series provides some sector-specific guidelines, e.g. for cloud computing or telecommunications. In the context of automation technology, the sector-specific guideline **[ISO_27019]** is of interest. It offers a guideline based on [DIN_EN_ISO_IEC_27002] and applied to process control systems used by the energy supply industry to control and monitor the production or generation, transmission, storage and distribution of electrical energy, gas, oil, and heat as well as to control the associated supporting processes are used. This includes in particular the following:

- Centralized and decentralized process control, monitoring and automation technology as well as information systems used for their operation, such as programming and parameter setting devices;
- Digital controllers and automation components such as control and field devices or programmable logic controllers (PLCs), including digital sensor and actuator elements;
- All other supporting information systems that are used in the area of process control, e.g. for additional tasks of data visualization as well as for control, monitoring, data archiving, history logging, reporting and documentation;
- Communication technology that is used in process control, e.g. networks, telemetry, remote control applications and remote-control technology;
- Components of the Advanced Metering Infrastructure (AMI), e.g. smart meters;
- Measuring devices, e.g. for emission values;
- Digital protection and safety systems, e.g. protective relays, safety PLCs, emergency shutdown system;
- Energy management systems, e.g. by Distributed Energy Resources (DER), electrical charging infrastructure in private households, residential buildings or industrial customer facilities;
- Distributed components of smart grid environments, e.g. in energy grids, in private households, residential buildings or industrial customer facilities;
- All software, firmware and applications that are installed on the above systems, e.g. DMS (Distribution Management System) applications or OMS (Outage Management System);
- All premises in which the above-mentioned devices and systems are installed;
- Remote maintenance systems for the systems mentioned above.

[ISO_27019] does not apply to the process control domain of nuclear facilities. This domain is covered by IEC 62645. [ISO_27019] also contains the requirement to adapt the processes for risk assessment and treatment described in [DIN_EN_ISO_27001] to the sector of energy supply companies.

2.1.5. Further literature on ISO 27000

It is recommended that newcomers to the ISO 27000 series of standards first familiarize themselves via a textbook and not directly via the standards. For example, [BRE2020], [KER2020] can be used for this purpose. Readers who have a background in risk management

are additionally recommended to read [KLI2015]. An online overview of the standards with brief descriptions of the individual standards can be found under [ISE2020].

2.2. The IEC 62443 series of standards

The IEC 62443 series of standards is developed by the International Electrotechnical Commission (IEC) and the International Society of Automation (ISA). The first work on the standard was started in the ISA SP99 working group and is currently being continued in a cooperation between IEC and ISA. Therefore, many documents still contain references to ISA working groups and documents.

Based on the models and requirements of the ISO 27000 series of standards, the IEC 62443 series of standards takes into account the special requirements of IT security in the production area. Figure 3 shows the structure of the series of standards.

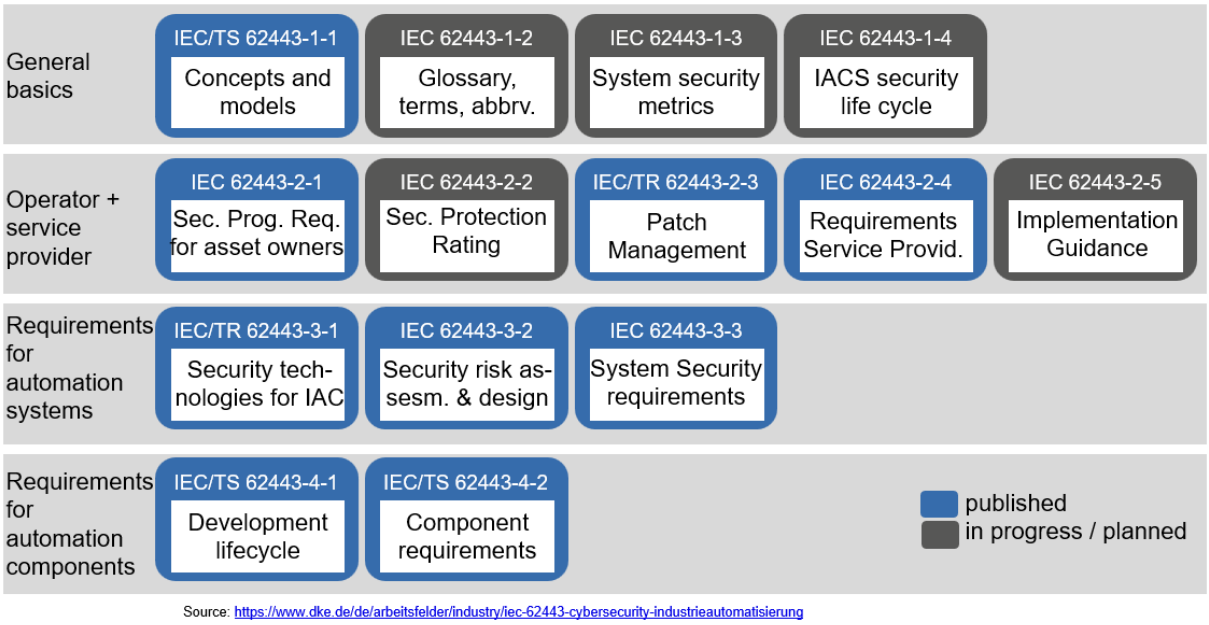

Figure 3: Parts of IEC 62443, based on [DKE2020]

The IEC 62443 series of standards consists of four main areas, which are presented in the following chapters, including the associated standards.

2.2.1. General basics

Figure 4 shows the IEC 62443 standards of the part "General principles. The parts highlighted in gray are currently still being processed and not published.

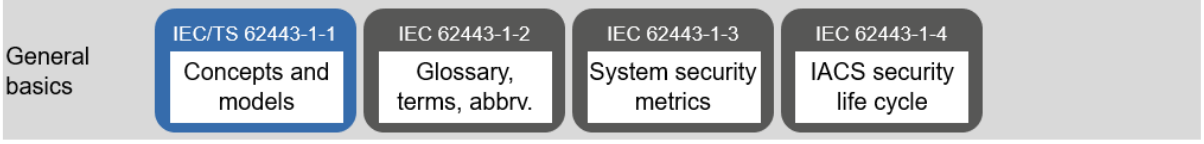

Figure 4: IEC 62443 - Part 1 General principles based on [DKE2020]

[IEC_62443-1-1] is a technical specification which defines the terminology, concepts and models for the security of industrial automation and control systems (IACS). It forms the basis for the other standards in the IEC 62443 series. This standard includes information on:

- Risk assessment
- Security program maturity
- Policies
- Zones and conduits
- Models
- Reference architecture

Part [IEC_62443-1-2] defines all terms that are used in the standards. Part [IEC_62443-1-3] defines metrics for evaluating IT security, part [IEC_62443-1-4] describes the security lifecycle and use cases. All three parts have not yet been published and are only available as draft to members of the working group.

2.2.2. Operators and service providers

Figure 5 shows the "Operators and service providers" part of the IEC 62443 series of standards.

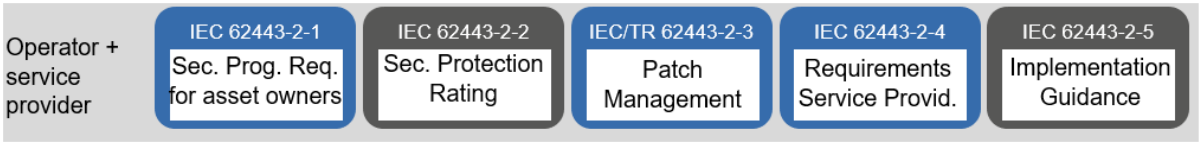

Figure 5: IEC 62443 - Part 2 Operators and service providers based on [DKE2020]

This part describes the IT Security Management System and thus defines the organization of IT security, followed by implementation aids.

Part **[IEC_62443-2-1]** describes requirements for an IT Security Management System, e.g. the

- Definition of security procedures
- Risk management
- Definition of training requirements
- Business continuity plans
- Access control
- Improvement process
- etc.

Part **[ISA_62443-2-2]** provides information on how and in which areas these procedures are to be implemented. It specifies a framework for evaluating an IACS's degree of protection. It contains a procedure for combining the evaluation of both organizational and technical security measures in numerical values, the so-called "Protection Level". The framework forms the structure for the evaluation of the Defense-in-Depth-strategy of the IACS in operation, on the basis of the technical and organizational requirements which are specified in other documents of the IEC 62443 series of standards. [DKE2020]. This part is currently only available in draft form.

Updating the software of automation systems, or patching, is of particular importance because improper procedures can lead to operational disruptions. The series of standards therefore devotes a separate part to patch management **[IEC_62443-2-3]**.

Part **[DIN_EN_IEC_62443-2-4]** deals with the use of service providers for commissioning and service from the point of view of IT security. "It defines requirements for IT security guidelines, procedures and practices that are applicable to suppliers of industrial automation systems during the life cycle of their products, as well as to maintenance service providers. In particular, it addresses integrators who combine technical solutions to form an overall system." [DKE2020] This standard is available in English and German.

The **[IEC_62443-2-5]** is planned and should contain implementation instructions for operators. The author has not yet received any drafts for this standard part.

2.2.3. Requirements for automation systems

Figure 6 shows the parts of the standard which describe the requirements for automation systems.

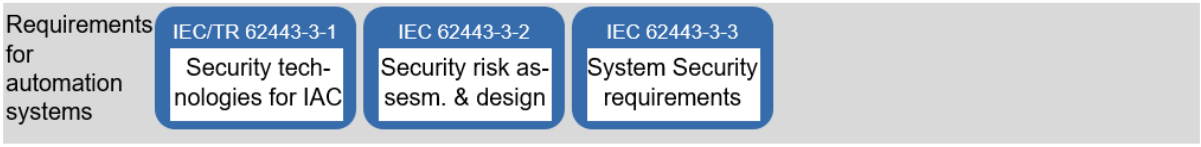

Figure 6: IEC 62443 - Part 3 Requirements for automation systems based on [DKE2020]

Part [IEC_62443_3_1] first describes the underlying technologies such as authentication, encryption, filtering and logging. Part [IEC_62443_3_2] describes the entire security analysis process and, based on this, the partitioning of a system into zones (isolated areas) and conduits (secure connections between areas). The target is to divide an automation system into subareas, which in turn are isolated from one another. Part [IEC_62443-3-3] describes specific requirements for automation systems in the form of basic requirements (Foundational Requirements). These Foundational Requirements (FR) define the IT security cornerstones of the system.

- Identification / authentication control (IAC)
  - Recording of all users (people, software, components)
- Use control (UC)
  - Enforcing user access rights
- System Integrity (SI)
  - Preventing manipulation of the IACS
- Data confidentiality (DC)
  - Securing data in communication channels and memories
- Restricted data flow (RDF)
  - Zoning and protected communication channels
- Timely response to events (TRE)
  - Fast notification of entities about IT security incidents
- Resource Availability (RA)
  - Ensuring availability of resources

This part of the standard provides specific information for planners and operators of automation systems with regard to specific technical measures.

These measures are assigned to so-called security levels (SL).

Table 1: Security level according to [DIN_EN_IEC_62443-4-1]

SL	Description
1	Preventing the unauthorized disclosure of information through eavesdropping or accidental exposure.
2	Preventing the unauthorized disclosure of information to a unit which actively searches for it using simple means and little effort, general skills and little motivation.
3	Preventing the unauthorized disclosure of information to a unit which actively searches for it using sophisticated means and moderate effort, IACS-specific skills and moderate motivation.
4	Preventing the unauthorized disclosure of information to a unit which actively searches for it using sophisticated means and considerable effort, IACS-specific skills and high motivation.

The standard specifies the levels SL1 (low requirements) to SL4 high requirements. Depending on the necessary degree of protection for the system, the requirements can be selected according to the desired security level.

2.2.4. Automation component requirements

Figure 7 shows the standard parts that define the requirements for the development process and the components of the automation system. These parts are intended for manufacturers of automation systems.

Figure 7: IEC 62443 - Part 4 Requirements for components of automation systems based on [DKE2020]

Part **[DIN_EN_IEC_62443-4-1]** defines the development process that must be observed when developing components for automation technology.

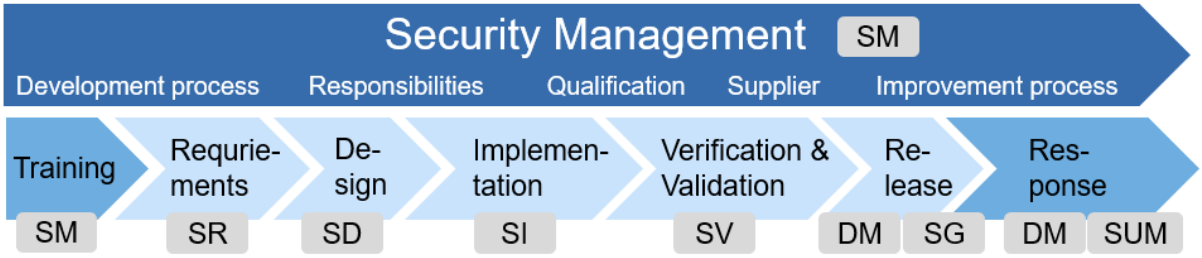

Figure 8: Safe development life cycle, based on [WAL2020]

Figure 8 shows the secure development life cycle described in the standard. It can be seen that this extends over all phases of the development process. Manufacturers of automation components can use the implementation of this standard to build the product development life cycle in accordance with the security-by-design approach and thus lay the basis for the certification of components. The abbreviations in the gray boxes correspond to the requirement classes from the respective parts of the standard. For an organization structured in this way, maturity levels from 1 to 4 are assigned.

Part **[DIN_EN_IEC_62443-4-2]** describes the technical requirements for the components of automation systems, application and functions. The structure of the requirements follows [DIN_IEC_62443-3-3], but it describes the requirements to be met by components. A distinction is made between Component Requirements (CR) and Requirement Enhancements (RE). These requirements are derived from the System Requirements (SR).

The types of components of an IACS specified in this document are

- Software applications,
- Host devices,
- Embedded devices and
- Network components.

The majority of CRs and REs apply to all four component types and are grouped into a single Component Requirement (CR). Some CRs and REs only apply to a certain type of component. With [ZVE2017], the ZVEI gives manufacturers of automation components an introduction to the subject.

2.2.5. *Assigning IEC 62443 standard parts to stakeholders in the security process*

Figure 9 provides an overview of the stakeholders in the IT security process and the assignment of the IEC 62443 standard parts to them.

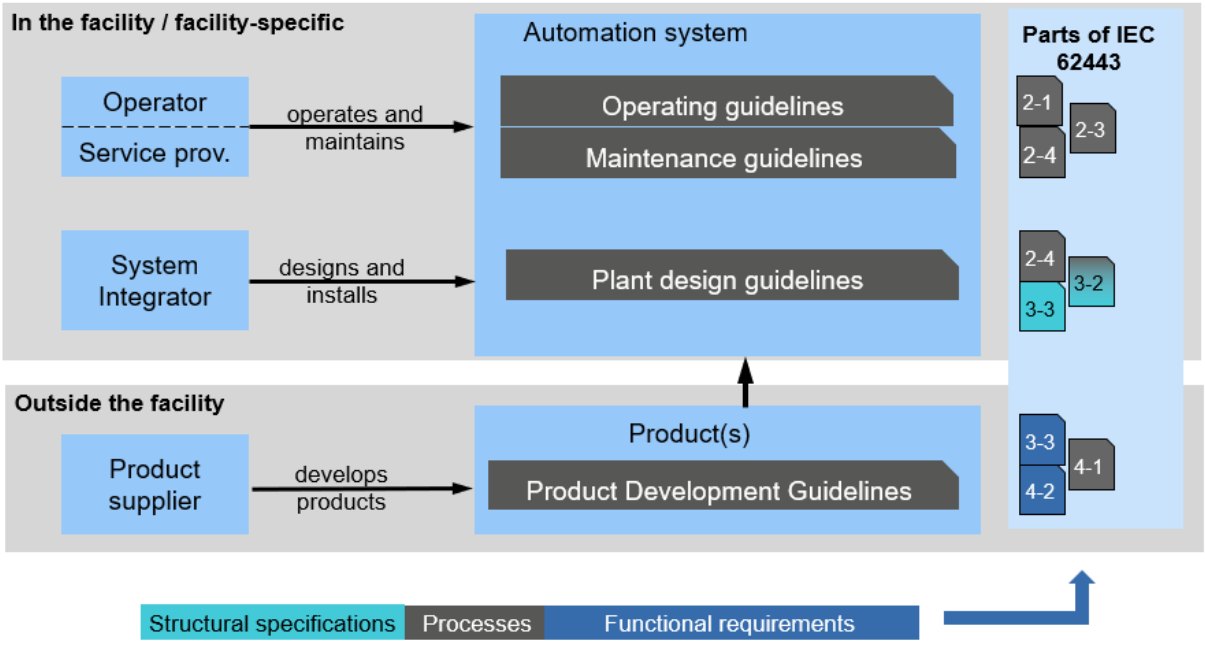

Figure 9: Assignment of the ICE 62443 standard parts to stakeholders in the security process (based on [ISA_62443-2-2])

The role of operator/service provider is responsible for the operation and maintenance of a production facility. For these stakeholders, the guidelines for operation and maintenance are most relevant, especially those standard parts regulating the establishment and operation of the ISMS [IEC_62443-2-1] and the integration of service providers [IEC_62443-2-4]. Part [IEC_62443-2-3], which regulates the updating of the control system software (patch management), is also relevant for operators.

The role of system integrator designs and installs the automation system. Here, the standard part [DIN_IEC_62443-3-3] is relevant, which makes specifications with regard to the structure and partitioning of the system. Part [DIN_EN_62443-3-2] can also be consulted for security risk assessment and system design. If the planning process is carried out by a service provider, the part [IEC_62443-2-4], which describes requirements for service providers, must also be observed. If the facility operator himself carries out the planning work, the standards mentioned in this section also apply accordingly to the operator in his role as production facility planner.

The third role is that of product suppliers. For these suppliers, first and foremost [DIN_EN_IEC_62443-4-1] applies, which specifies the requirements for a secure development process (security by design). The requirements for products developed by the product supplier are described in part [DIN_EN_IEC_62443-4-2]. Since the requirements in this standard are derived from system requirements, the product supplier should also know and observe these system requirements [DIN_IEC_62443-3-3].

2.2.6. Further literature on IEC 62443

The standards of the IEC 62443 series have so far only been partially published. The majority of the series of standards is at least available in draft form. The current status of the work and the release status of the standard parts can be viewed under [ISA2020]. The status of the German translations can be found in [DKE2020].

[KOB2021] gives an overview of the IEC 62443 series of standards and explains the relationships between the parts of the standard. This book provides a compact and quick introduction to the standard. In their book, [GUN2018] give detailed information on the introduction of IEC 62443.

The industry associations ZVEI [ZVE2017] and VDMA [VDM2016] provide guidelines for the implementation of IEC 62443. The ZVEI from the manufacturer's point of view, the VDMA from the operator's point of view.

3. Differentiation of the IT security standards

Now that the two series of standards IEC 62443 and ISO 27000 have been described in detail in the previous chapters, a differentiation should be made between the two standards with regard to their applicability in the production area. It should be noted that IT security is a company-wide issue and that the production area therefore cannot be viewed separately. Nevertheless, IT security requirements in the production area are different from the ones in the office area. Therefore, the following chapter first describes these requirements and then distinguished the areas IT (Information Technology) and OT (Operational Technology) from one another.

3.1. Differentiation of the OT and IT application domains

In the following, the IT and OT application domains are initially delimitated against one another in order to derive specific requirements for IT security management in the further course of the chapter. Table 2 defines the terms IT and OT and shows application examples.

Table 2: Differentiation of the IT and OT domains

Domain	Definition according to Gartner Group [GAR2021]	Application examples
IT	"IT" is the common term used to describe the full range of information processing technologies, including software, hardware, communication technologies and related services. In general, IT does not include embedded technologies provided that they do not generate data for corporate use.	• Client systems of staff • Laptops • Web server • Mail server • SAP systems • File server • Networks
OT	Operational technology (OT) is hardware and software that detects or causes a change by directly monitoring and/or controlling industrial equipment, facilities, processes and events.	• Programmable logic controllers • Display systems (touch panels) • Production control server • Industrial robots • Remote IO systems • Real-time networks

Having defined the two application domains, the requirements with regard to IT security will now be considered. First of all, it must be considered that different terms are used within the two domains. Figure 10 shows a differentiation of the terms.

Protection of IT in the office area	Protection of IT in the production area	Protection of personal data
IT security Information security	Cyber security OT security AT security ICS security	Data protection Data security

Figure 10: Differentiation of the terms IT / OT security

It can be seen that the terms "information security" or “IT security” are used when talking about the protection of IT in the office area. The term “information security” can refer to the protection of information in general. This includes, for example, intellectual property. [ISO_27000] uses the term “information security” and defines it as ensuring the confidentiality, integrity and availability of information. The term “IT security” is a partial aspect of information security. This concerns the protection of technical systems. The terms "cyber security" or "ICS security" [BSI_2014] are often used when talking about production facilities. This focuses on the security of operational facilities (OT). The term “data protection” shall only be mentioned for the sake of completeness but is of no relevance here. As there are different areas of application of IT and OT, different requirements with regard to IT and OT security are derived from this. These are shown in Table 3.

Table 3: IT and OT security requirements (based on [FLA2019])

	IT	OT
	Security properties	
Prioritization of security requirements	Confidentiality, integrity, availability, non-repudiation	Availability, integrity, non-repudiation, confidentiality
Availability	Important, but not critical	Critical
Integrity	Important	Important
Confidentiality	Critical	Not critical
	Technology	
Real-time behavior	Desired but not critical (Quality of Service)	Critical for the function of the production facility
Technology used	Homogeneous	Very heterogeneous, different protocols, embedded systems.
	Operation	
Useful life	3... 5 years	Sometimes more than 20 years
Software update	Automatically	Critical: In some cases only during system downtime, preliminary test of the updates required, approval of the updates by control system manufacturer required
Outsourcing	Common	Common for planning, establishment and maintenance, not for operation.
	Security management	
Risk analysis	Global, company-wide	Facility-related
User authentication and access rights	Personalized, centrally managed	Often role-based, shift access for user groups
Security awareness	High	Poorly developed
Use of anti-virus software	Common	Problematic, often out of date

The information in Table 3 shows that there are different requirements in terms of IT security for the IT and OT areas. As a result, in addition to the ISO 2700 series, the IEC 62443 series of standards has been developed for the IT security of production facilities, which addresses these special requirements.

3.2. Differences and similarities between ISO 27000 and IEC 62443

Having described the different requirements of IT and OT in the previous chapter, the differences and similarities shall now be considered and mapped to the two series of standards ISO 27000 and IEC 62443.

The **ISO 27000 series** describes the establishment and operation of an IT security management system (ISMS). The series of standards addresses information security in general and does not differentiate between data in IT systems or intellectual property. The standard [DIN_EN_ISO_27001] should be regarded as a basic standard which defines the essential requirements for the organization of IT security, such as planning, responsibilities, risk assessment, communication, resources, internal audit. It can therefore be said that it focuses on the organization and process-related aspects of IT security. [DIN_EN_ISO_IEC_27002] defines specific requirements for IT security, such as access control, network security, separation of networks, etc. One focus of the series of standards is the monitoring and evaluation of the ISMS [ISO_27004] and its certification [ISO_27007]. The standard is generic and can be used for IT applications as well as for OT. However, the standard does not make any specific reference to the requirements of OT, as described, for example, in Table 3. Part [DIN_IEC_27019], however, is an exception as it focuses specifically on energy supply systems.

The **IEC 62443 series** focuses on the protection of industrial automation systems and therefore belongs to the area of Operational Technology (OT). Special features of OT are considered. Requirements relating to service providers [DIN_EN_IEC_62443-2-4], for instance, are taken into account, as well as patch management in production facilities in part [IEC_62443-2-3]. The aspect of establishing and operating an ISMS is also included in the series of standards [IEC_62443-2-1], but the focus is on specific technical requirements for automation systems [IEC_62443-3-3] and the components of automation systems [DIN_EN_IEC_62443-4-2], the latter being aimed at manufacturers of automation components.

Both series of standards have similarities. It can be seen that the basic concepts and technologies can be found in both series of standards. It should be noted, however, that the IEC 62443 series of standards has a clear focus on automation technology, whereas the ISO 27000 series is more process-oriented and generic. See also [KOH2018].

Focus on organization	1. Management commitment. 2. Organization of responsibilities and processes. 3. Directive/ Guideline. 4. Staff. 5. Knowledge.
Focus on technology	6. Identify, evaluate and protect the assets: 1. Automation systems. 2. Networks. 7. External access.
Focus on organization	8. Data backup. 9. Disruptions and failures. 10. IT security incidents.

Figure 11: Aspects of IT security in production facilities

Figure 11 shows the various aspects of IT security in production facilities. It can be seen that the focus here is on organizational aspects on the one hand and on technical aspects on the other. For tasks with a focus on technology, it makes sense to use the IEC 62443 series of standards because there is a clear focus on the requirements of automation technology. For tasks in the production area with a focus on organization, either the [IEC_62443-2-1] or the

ISO 27000 series of standards can be used. If an ISMS according to ISO 27000 is already in place for IT, it makes sense to also treat the organizational aspects in OT accordingly. The experiences from such a combined use of both parts of the standard at a power distribution network operator are described in [MON2019].

A comparable approach is described in [FRI2019]. This document also describes the joint use of both series of standards in the field of power distribution.

Further information on the organization of IT security can also be found in [NIE2018]. When considering these standards, the question of certification of an ISMS or products is often raised. The certification, e.g. of automation components according to [DIN_EN_IEC_62443-4-2] is a basis for ensuring the IT security of a production facility according to [DIN_IEC_62443-3-3].

3.3. Overlapping of the requirements of IEC 62443 and ISO 27000

The previous chapters have shown that the two series of standards under consideration, IEC 62443 and ISO 27000, overlap. An illustration of the requirements of both series of standards (mapping) is available from different sources. For more information, see

- [ÖST2020] Mapping Table of ICT Security Standards and Cyber Security Best Practices
- [BSI2013] ICS Security Compendium
- [ENI2017] ENISA Mapping of OES Security Requirements to Specific Sectors.

4. Summary and recommendation

The following recommendations can be derived from the previous chapters:

1.) If the company already has an ISMS according to ISO 27000, the organizational processes in the production area should follow these concepts in order to achieve a uniform process landscape.
2.) If no ISMS is in place and only the production area is to be considered, the ISMS can be implemented according to [IEC_62443-2-1].
3.) Small and medium-sized companies, for which an ISMS according to ISO 27000 may be too complex, should consider the use of a simplified ISMS, e.g. according to BSI Baseline Protection [BSI_200-1] or [VDS_10000] and [VDS_10020].
4.) The specific technical aspects of IT security in the production area should preferably be developed according to [DIN_IEC_62443-3-3].
5.) For the operational aspects of IT security in the production area, [IEC_62443-2-3] and [DIN_EN_IEC_62443-2-4] can also be used.
6.) Systems belonging to critical infrastructure as stated in the IT Security Act [ITSichG2015] must be considered separately, as recurring certification is necessary here, which usually requires an ISMS in accordance with ISO 27000.

5. Appendix: Application to a wastewater treatment plant

This appendix shows by way of example the concrete application of the previous considerations to a wastewater treatment plant. First of all, it is defined whether a system belongs to a critical infrastructure or not. The document then describes the industry standards applicable in Germany for the water and wastewater sector. The chapter closes with a proposal for an assessment procedure for wastewater treatment plants.

5.1. Risk assessment for wastewater treatment plants

With regard to the threat to the IT security of wastewater treatment plants, there are already publications describing known incidents:

- An attack on a wastewater treatment plant in Australia was documented as early as 2000 [SLA2008]. Here, an external consultant misused the access codes to wireless transmission systems known to him to compromise the system.
- In 2018, security researchers described that they had been able to gain unrestricted online access to wastewater treatment plants with administrator rights [TRE2018].
- The KRITIS sectoral study by the BSI [BSI2015] mentions incidents at the Lübeck municipal utilities in 2014 and an attack on the water supply of the city of Haifa in 2013.
- In a report from 2020, the consulting firm Alpha Strikes found more than 30 vulnerabilities in areas of wastewater and information technology of the "Berliner Wasserbetriebe" municipal water utility [JAN2020].
- [NEU2020] states that a majority of utilities are not adequately protected.

In summary, it can be said that wastewater systems and the associated control centers are exposed to a risk with regard to IT security. This applies in particular when remote access is used for external access.

The attacks on wastewater treatment plants are based on two main attack vectors:

- External attacks:
    - Targeted attacks from outside, e.g. with the aim of disrupting data communication or intruding into the network.
    - Random external attacks, e.g. by scanning address ranges to find specific components.
    - Attack on remote control systems.
    - Attack via systems for remote maintenance or remote control of the plant.
    - Breaking into the facility.

- Internal attacks:
    - Opening compromised email attachments, spread of malware to the automation network.
    - Inattention or lack of know-how by staff, e.g. when installing software updates.
    - Connection of laptops / USB sticks from external staff with components of the system.
    - Insiders who intentionally want to compromise the facility.

Both attack vectors must be considered in a risk assessment.

5.2. Critical infrastructure or not?

In its glossary, the BSI defines a critical service as follows:

"Critical services are important, sometimes vital, goods and services for the population. If these critical services were impaired, there would be considerable supply bottlenecks, disruptions to public safety or comparable dramatic consequences." [BSI2021a].

These critical services are provided through certain facilities, such as power plants, waterworks, port facilities or airports. These facilities are commonly referred to as critical infrastructure. The BSI defines critical infrastructures as follows:

"Critical infrastructures are organizations and facilities with great importance for the state community, whose failure or impairment would result in lasting supply bottlenecks, significant disruptions to public safety or other dramatic consequences. In Germany, the following sectors (and industries) are classified as Critical Infrastructures:

- *Transport and traffic (aviation, maritime shipping, inland shipping, rail traffic, road traffic, logistics)*
- *Energy (electricity, mineral oil, gas)*
- *Information technology and telecommunications (telecommunications, information technology)*
- *Finance and insurance (banking, insurance companies, financial service providers, stock exchanges)*
- *State and administration (government and administration, parliament, judicial institutions, emergency and rescue services including disaster control)*
- *Nutrition (food industry, food trade)*
- *Water (public water supply, **public wastewater disposal**)*
- *Health (medical care, drugs and vaccines, laboratories)*
- *Media and culture (broadcasting (television and radio), printed and electronic press, cultural assets, symbolic buildings*)" [BSI2021a]

The BSI KRITIS regulation [BSI-KritisV_2016] defines the size from which a public wastewater treatment plant is considered part of the critical infrastructure. The following figures are assumed:

- Wastewater produced: 44 m^3 per person per year and
- Control threshold: 500,000 people catered for

This results in

- 44 m^3/year · 500,000 = 22 million m^3/year

This means that all wastewater treatment plants with a throughput of 22 million m^3/year or more are classified as critical infrastructure. Further details on the calculation and evaluation of connected plants can be found in [BSI-KritisV_2016]. This regulation was updated in 2017 [BSI-KritisV_2017]. However, the update has had no effect on the above thresholds. With the passing of the IT Security Act 2.0 [IT-SIG_2.0] and with an update of the KRITIS regulation, a reduction in the thresholds is to be expected.

The Federal Statistical Office records wastewater treatment plants according to size in [STA2016]. However, only up to an annual wastewater volume of 6 million m^3/year. Of the 9,105 wastewater treatment plants in Germany, 276 have an annual wastewater volume of 6 million m^3/year or more. This corresponds to approximately 3% of the facilities. It can be deduced from this that the number of wastewater treatment plants that belong to the critical infrastructure will be even lower, since the threshold for this is 22 million m^3/year. This assessment is consistent with figures from the water supply sector. There, only 0.82% of the facilities are considered critical infrastructure [NEU2020].

According to [BSI-KritisV_2016], [ITSichG2015] and [BSIG_2020], affected municipal wastewater disposal companies must meet the following requirements:

- The KRITIS operator must set up a contact point via which it can be contacted at any time by the BSI.
- Significant IT security incidents that could lead or have led to a failure or impairment of the disposal of the wastewater must be reported to the BSI. The BSI maintains a reporting office for this purpose.
- The KRITIS operator must have secured its IT according to the state of the art.
- The KRITIS operator must prove to the BSI that the IT security level has been met through security audits, inspections or certifications at least every two years.

Further information with questions and answers for operators of critical infrastructures can be found in [VKU2016] and in [BSI2017].

5.3. Applicable norms and standards for water / wastewater technology

In this chapter, the applicability of the ISO 27000 and IEC 62443 series of standards to wastewater management systems shall be examined. In addition, an industry-specific standard for water/wastewater management is also considered.

5.3.1. Applying the ISO 27000 series of standards to wastewater treatment plants

The ISO 27000 series of standards can be used for the protection of wastewater systems. In particular, the establishment of an information security management system according to [DIN_EN_ISO_27001] must be observed. The technical requirements for IT security can be implemented according to [DIN_EN_ISO_IEC_27002]. It should be noted, however, that these are generic requirements that are not aimed specifically at automation systems. The only standard with a reference to automation systems is [ISO_27019]. This standard is aimed at power generation and distribution facilities but can also be used analogously for wastewater facilities.

The BDEW whitepaper [BDE2018] maps the requirements from [DIN_EN_ISO_IEC_27002] to the components of a wastewater treatment plant.

Operators of critical infrastructures must document via regular audits that the state of the art in terms of IT security is applied. The ISO 27000 series of standards or the industry-specific security standard described in Chapter 5.3.3 is generally used here.

For operators of small wastewater treatment plants that are not part of the critical infrastructure, the application of the ISO 27000 series of standards is challenging, as it is a very comprehensive set of standards.

5.3.2. Applying the IEC 62443 series of standards to wastewater treatment plants

The IEC 62443 series of standards focuses on automation systems. Part [IEC_62443-2-1] describes the requirements for an IT Security Management System. Part [IEC_62443-2-3] deals with patch management, part [DIN_EN_IEC_62443-2-4] with the use of service providers for commissioning and service from the point of view of IT security. It can be seen that this series of standards focuses more strongly on the conditions in a production environment, such as continuous operation.

Part [IEC_62443-3-3] describes specific requirements for automation systems in the form of basic requirements (Foundational Requirements). These Foundational Requirements (FR) define the IT security cornerstones of the system. Parts [DIN_EN_IEC_62443-4-1] and [DIN_EN_IEC_62443-4-2] define requirements for the suppliers of automation components.

In summary, it can be stated that the IEC 62443 series of standards provides all the necessary components (ISMS, risk assessment, technical requirements for systems and components). Operators who mainly focus on the automation system can proceed in a targeted manner without having to deal with the complexity of the ISO 27000 series. Experience reports on the

protection of wastewater treatment plants in connection with IEC 62443 can be found, for example, in [CHR2019] and [TEB2020]. It should be noted, however, that an ISMS must be planned in any case.

5.3.3. Use of the industry-specific security standard for water/wastewater (B3S WA)

The IT Security Act [ITSichG2015] defines in §8a (2):

"Operators of critical infrastructures and their industry associations can propose industry-specific security standards to guarantee the requirements referred to in paragraph 1. Upon request, the Federal Office will determine whether these are suitable for ensuring the requirement referred to in paragraph 1."

The industry-specific security standard for water/wastewater (B3S WA) was created on the basis of this definition. It consists of the following parts:

- Information sheet on IT security, industry standard for water/wastewater [DWA-M_1060]
- IT security guidelines - web application for Information sheet DWA-M 1060 [DWA2020]
- Orientation aid for the verification procedure [DWA2018]

Information sheet [DWA-M_1060] initially defines the area of application and the essential terms. This is followed by the definition of the desired protection goals of availability, integrity, authenticity and confidentiality. According to the information sheet, this means in detail:

- Failures/downtimes of information technology systems, components or processes are avoided, and the relevant data can be accessed at any time.
- Unauthorized modification of the information technology systems, components or processes and their data is prevented.
- The correct functioning of the systems and the integrity of data, the authenticity, verifiability and trustworthiness of data and their origin are guaranteed.
- The information is protected against unauthorized disclosure.

In a next step, the information sheet describes the requirements for an Information Security Management System (ISMS) and the requirements for business continuity management. This is followed by the description of the risk assessment with the individual steps: Risk identification, risk analysis, risk assessment and responsibilities of the operator. The following part of the information sheet then describes the measures to minimize risk.

The IT security guidelines supplementing the information sheet describe based on use cases both the threats to IT security and the corresponding measures to be taken for all types of facilities in accordance with [BSI-KritisV_2016] in the water sector. The use cases describe the possible IT systems/IT configurations and other conditions regarding the IT equipment of facilities. [DWA-M_1060]. The basis for these cases is the BSI basic protection compendium [BSI2021b].

The industry-specific standard can be applied both to wastewater facilities belonging to critical infrastructure and to conventional wastewater facilities. Experience reports on the application of the standard can be found in [FIE2020] and [TEN2018].

The BSI has published guidelines for the application of the standard [BSI2018]. This document deals in particular with the parallel use of ISO 27001 and the industry standard. At the end of the document, the BSI provides a detailed reference table for comparing the alternatives.

6. References

6.1. List of figures

6.2. List of tables

6.3. Literature cited

[BDE2018] BDEWBDEW Bundesverband der Energie- und Wasserwirtschaft e.V. Whitepaper Requirements for secure control and telecommunication systems. https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf.

[BRE2020] Brenner, Michael; gentschen Felde, Nils; Hommel, Wolfgang Practical Guide ISO/IEC 27001. Information security management and preparation for certification. Carl Hanser Verlag GmbH & Co. KG, Munich, 2020.

[BSI_200-1] Federal Office for Information Security (BSI) BSI Standard 200-1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2.

[BSI_2014] Federal Office for Information Security ICS Security Compendium. Test recommendations and requirements for component manufacturers. As at 11/19/2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf;jsessionid=DB019AA1A22E666BE17192033909CB6D.2_cid359?__blob=publicationFile, 10/26/2014.

[BSI2013] Federal Office for Information Security ICS Security Compendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile, 06/05/2014.

[BSI2015] Federal Office for Information Security (BSI) KRITIS sectoral study on nutrition and water. https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_Ernaehrung_Wasser.pdf?__blob=publicationFile.

[BSI2017] Federal Office for Information Security (BSI) Protection of critical infrastructures through the IT Security Act and UP KRITIS. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf;jsessionid=E0CD6CAD7BAE814DD7140BE30ED859D5.internet081?__blob=publicationFile&v=1.

[BSI2018] Federal Office for Information Security (BSI) Use of the industry-specific security standard water/wastewater (B3S WA) in affiliated companies. Initial situation – Analysis – Recommendations. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/B3S_WA_Analyse_Empfehlungen_pdf.pdf?__blob=publicationFile&v=3.

[BSI2021a] Federal Office for Information Security (BSI) Protection of Critical Infrastructures. Glossary. https://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/glossar_node.html;jsessionid=CA30D56F33392F5444A3F945140B4B85.1_cid345.

[BSI2021b] Federal Office for Information Security (BSI) IT Basic Protection Compendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6.

[BSIG_2020] Law on the Federal Office for Information Security. BSI Act-BSIG, 2020.

[BSI-KritisV_2016] Ordinance on determining critical infrastructures according to the BSI Act (BSI Kritis Ordinance). BSI-KritisV, 2016.

[BSI-KritisV_2017] First regulation amending the BSI-Kritis regulation. BSI Kritis Vo, 2017.

[CHR2019] Christ, Jochen Cybersecurity for Water Management: Protect what is important. In Automation Blue, 2, 2019; Pp. 56–59.

[DIN_EN_62443-3-2] DKE-German Commission for Electrical Engineering, Electronics Information Technology DIN and VDE, DIN German Institute for Standardization e. V, DIN EN 62443-3-2 (VDE 0802-3-2) Security for industrial automation systems - Part 3-2: Security risk assessment and system design (IEC 65/690/CDV:2018); German and English version prEN 62443-3-2:2018. Beuth Verlag, 2018.

[DIN_EN_IEC_62443-2-4] DKE German Commission for Electrical, Electronic and Information Technologies in DIN and VDE, DIN EN IEC 62443-2-4 (VDE 0802-2-4): 2020-07 Security for industrial automation systems - Part 2-4: Requirements for the IT security program of service providers for industrial automation systems (IEC 62443-2-4:2015 + Cor.:2015 + A1:2017); German version EN IEC 62443-2-4:2019 + A1:2019.

[DIN_EN_IEC_62443-4-1] DKE-German Commission for Electrical Engineering, Electronics Information Technology DIN and VDE, DIN German Institute for Standardization e. V, DIN EN IEC 62443-4-1 (VDE 0802-4-1) IT security for industrial automation systems - Part 4-1: Life cycle requirements for secure product development (IEC 62443-4-1 2018); German version EN IEC 62443-4-1 2018. Beuth Verlag, Berlin, 2018.

[DIN_EN_IEC_62443-4-2] DKE-German Commission for Electrical Engineering, Electronics Information Technology DIN and VDE, DIN EN IEC 62443-4-2 IT security for industrial automation systems - Part 4-2: Technical security requirements for components of industrial automation systems (IACS) (IEC 62443-4-2:2019); German version EN IEC 62443-4-2:2019, 2019.

[DIN_EN_ISO_27000] DIN Standards Committee Information Technology and Applications (NIA), DIN EN ISO/IEC 27000:2020 Information technology - Security procedures - Information security management systems - Overview and terminology (ISO/IEC 27000:2018); German version EN ISO/IEC 27000:2020, 2020.

[DIN_EN_ISO_27001] DIN Standards Committee Information Technology and Applications (NIA), DIN ISO/IEC 27001:2017 Information technology - Security procedures - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1: 2014 and Cor 2:2015); German version EN ISO/IEC 27001:2017, 2017.

[DIN_EN_ISO_IEC_27002] DIN German Institute for Standardization e. V, DIN ISO/IEC 27002:2017 Information technology - Security procedures - Guidelines for information security measures (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015); German version EN ISO/IEC 27002:2017, 2017.

[DIN_IEC_27019] DIN Standards Committee Information Technology and Applications (NIA), DIN ISO/IEC TR 27019 DIN SPEC 27019 Information technology - Secu-

rity procedures - Guidelines for the information security management of control systems of the energy supply based on ISO/IEC 27002 (ISO/IEC TR 27019:2014). Beuth Verlag, Berlin, 2015.

[DKE2017] DKE-German Commission for Electrical Engineering, Electronics Information Technology DIN and VDE German Standardization Roadmap for IT Security. Version 3. https://www.din.de/resource/blob/238492/39d3f201a42007061c8013c0b76cf530/deutsche-normungs-roadmap-it-sicherheit-version-3-0-data.pdf.

[DKE2020] DKE-German Commission for Electrical Engineering, Electronics Information Technology DIN and VDE EC 62443: The international series of standards for cybersecurity in industrial automation. https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung.

[DIN_IEC_62443-3-3] DKE-German Commission for Electrical Engineering, Electronics Information Technology DIN and VDE, DIN IEC 62443-3-3 (VDE 0802-3-3) Industrial communication networks - IT security for networks and systems - Part 3-3: System requirements for IT security and security levels (IEC 62443-3-3:2013 + Cor.:2014). Beuth Verlag, 2015.

[DWA2018] DWA German Association for Water Management, Sewage and Waste e. V. Industry-specific security standard for water/wastewater (B3S WA) - Information on the verification procedure according to § 8a (3) BSIG. https://de.dwa.de/files/_media/content/05_PUBLIKATIONEN/DWA-Regelwerk/Arbeitshilfen%20aus%20dem%20DWA-Regelwerk/Branchspezischer_Sicherheitsstandard_Wasser_Abwasser.pdf.

[DWA2020] DWA German Association for Water Management, Sewage and Waste e. V. IT security guidelines (Version 2.0 - 2020) Web application for information sheet DWA-M 1060. https://de.dwa.de/de/it-sicherheitsleitfaden.html.

[DWA-M_1060] DWA German Association for Water Management, Sewage and Waste e. V., DWA-M 1060 Information sheet on IT security, industry standard water/wastewater, 2017.

[ENI2017] ENISA European Union Agency for Network and Information Security Mapping of OES Security Requirements to Specific Sectors. https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/.

[FIE2020] Fiene, Hans-Jürgen Technical report: Implementation of the B3S security standard in the Langwiese wastewater treatment plant. In Automation Blue, 4, 2020.

[FLA2019] Flaus, Jean-Marie Cybersecurity of industrial systems. ISTE Ltd, London, UK, 2019.

[FRI2019] Fries, Steffen Cybersecurity in Industrial Environments -From requirements to solutions on the example of Digital Grid. http://www.iaria.org/conferences2019/filesSECURWARE19/SteffenFries_Tutorial_SECURWARE.pdf.

[GAR2021] Gartner Inc. Gartner Glossary Information Technology. https://www.gartner.com/en/information-technology/glossary.

[GUN2018] Gunter, David G.; Medoff, Michael D.; O'Brien, Patrick C. Implementing IEC 62443. A pragmatic approach to cybersecurity. Exida, Sellersville, PA, 2018.

[IEC_62443-1-1] IEC- International Electrotechnical Commission, IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.

[IEC_62443-1-2] IEC- International Electrotechnical Commission, ISA-TR62443-1-2 Security for industrial automation and control systems - Master Glossary.

[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, 2014.

[IEC_62443-1-4] IEC- International Electrotechnical Commission, ISA-62443-1-4 Security for industrial automation and control systems Life Cycle and Use Cases, 2013.

[IEC_62443-2-1] IEC- International Electrotechnical Commission, IEC 62443-2-1-2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, 2010.

[IEC_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.

[IEC_62443-2-4] IEC- International Electrotechnical Commission, IEC 62443-2-4 Security for industrial automation and control systems – Network and system security – Part 2-4: Requirements for IACS solution suppliers., 2014.

[IEC_62443-2-5] IEC- International Electrotechnical Commission, IEC 62443-2-5 Implementation guidance for IACS asset owners, not released.

[ISA_62443-2-2] ISA - The International Society of Automation, ISA-62443-2-2 Security for industrial automation and control systems - Part 2-2: IACS security program rating, 2020.

[ISA2020] ISA - The International Society of Automation ISA99, Industrial Automation and Control Systems Security. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99.

[ISE2020] IsecT Ltd Overview on ISO 27000 standard series. https://www.iso27001security.com/html/iso27000.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_27003] ISO - International Standardization Organization, ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance, 2017.

[ISO_27004] ISO - International Standardization Organization, ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis, and evaluation, 2016.

[ISO_27005] ISO - International Standardization Organization, ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018.

[ISO_27006] ISO - International Standardization Organization, ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems, 2015.

[ISO_27007] ISO - International Standardization Organization, ISO/IEC 27007:2020 information security, cybersecurity, and privacy protection — Guidelines for information security management systems auditing, 2020.

[ISO_27019] ISO - International Standardization Organization, ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry, 2017.

[ITSichG2015] Act to increase the security of information technology systems (IT Security Act), 2015.

[IT-SIG_2.0] Second act to increase the security of information technology systems (IT Security Act 2.0). IT-SiG 2.0: Federal Law Gazette, 2021; Pp. 1122-1138.

[JAN2020] Jansen, Frank; Fiedler, Maria Waterworks inadequately protected against hacker attacks. https://www.tagesspiegel.de/politik/gutachten-warnt-vor-zirkenbruch-wasserbetriebe-gegen-hackerangriff-mangelhaft-geschuetzt/26045264.html.

[KER2020] Kersten, Heinrich; Klett, Gerhard; Reuter, Jürgen IT security management according to the new ISO 27001. ISMS, Risks, Indicators, Controls. Springer Fachmedien Wiesbaden, Wiesbaden, 2020.

[KLI2015] Klipper, Sebastian Information Security Risk Management. Risk management with ISO/IEC 27001, 27005 and 31010. Springer Vieweg, Wiesbaden, 2015.

[KOB2021] Kobes, Pierre Guide to Industrial Security. IEC 62443 in simple terms. VDE Verlag, Berlin, 2021.

[KOH2018] Kohl, Andreas; Bisale, Chaitanya Effective and efficient security based on international standards. In np, 9, 2018; Pp. 12-14.

[KRO2017] Kroeselberg, Dirk, Buchi, Frederic; Meulenbroek, Hans Cyber Security Tutorial Energy Automation and IEC 62443. https://www.pcic-library.com/sites/default/files/final/EUR17_63.pdf.

[MON2019] Montes Protela, Carlos; Hoeve, Maarten; Tan, Fook Hwa; Slootweg, Han Implementing an ISA/IEC-62443 and ISO/IEC-27001 OT Cyber Security Management System at Dutsch DSO Enexis: 25th International Conference on Electricity Distribution. Madrid, 3-6 June 2019. [CIRED], [Liège, Belgium], 2019; S. 1–5.

[NEW2020] Newer, Dietmar Cyber attacks: Most of the water suppliers are inadequately protected. https://www.handelsblatt.com/politik/deutschland/sicherheit-der-wasserversorgung-cyberattacken-grossteil-der-wasserversorger-nur-unzureichend-geschuetzt/26219428.html?ticket=ST-1111967-HqtoAWo6kfuH5auW4Xb5-ap6.

[NIE2017] Niemann, Karl-Heinz IT security in production facilities. An introduction for small and medium-sized businesses. https://doi.org/10.25968/opus-1135.

[NIE2018] Niemann, Karl-Heinz Organization of IT security in production. Ten steps for a secure production facility. In atp magazine, 11-12, 2018; Pp. 80-89.

[SLA2008] Slay, Jill; Miller, Michael Lessons Learned from the Maroochy Water Breach. In (Goetz, E.; Shenoi, Sujeet Hrsg.): Critical infrastructure protection. Springer, New York, NY, 2008; S. 73–82.

[STA2016] Federal Statistical Office Public Water Supply and Public Wastewater Disposal - Public Wastewater Treatment and Disposal -. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Umwelt/Wasserwirtschaft/Publikationen/Downloads-Wasserwirtschaft/abwasser-oeffnahm-2190212169004.pdf?__blob=publicationFile.

[TEB2020] Tebbe, Christopher Always up to date with IT security analyses: Digitization successfully implemented. Series of publications by the Mittelstand 4.0 Competence Center Hanover, Hanover, 2020; Pp. 14-22.

[TEN2018] Tenhart, Ludger B3S WA: Suitability determined, achieved in practice. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS_Tag_2018/B3S_WA_Eignung_feststellen_in_der_Praxis_angekommen.pdf?__blob=publicationFile&v=1.

[TRE2018] Tremmel, Moritz Per Web login to a wastewater treatment plant. https://www.golem.de/news/schwachstellen-aufgedeckt-per-weblogin-ins-klaerwerk-1812-138363.html.

[VDM2016] VDMA - Association of Machine and Plant Builders e. V. Security guidelines for mechanical and plant engineering The way through IEC 62443. http://pks.vdma.org/documents/105969/15311113/1479910314521_INS%20Security-Leitfaden%20VDMA_v1.0_WEB.pdf/b615dd92-3b84-4e93 -afb6-23f54fead723.

[VDS_10000] VdS Schadenverhütung GmbH, VdS 10000:2018-12 (02) Information security management system for small and medium-sized enterprises (SMEs), 2018.

[VDS_10020] VdS Schadenverhütung GmbH, VdS 10020:2018-01 (01) Cyber security for small and medium-sized enterprises (SMEs) - Guidelines for the interpretation and implementation of VdS 3473 for industrial automation systems, Cologne, 2018.

[VKU2016] Association of municipal companies e. V. Questions and answers on IT security legislation for water/wastewater. https://digital.vku.de/fileadmin/user_upload/vku_faq_it-sicherheit_wasser_abwasser.pdf.

[WAL2020] Waldeck, Boris Certified development process according to 62443-4-1 - Security by design, Online Seminar, Lemgo, 2020.

[ZVE2017] ZVEI - Zentralverband Elektrotechnik und Elektronikindustrie e. V. Orientation guidelines for manufacturers on IEC 62443. https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/April/Orientierungsleitfaden_fuer_Hersteller_IEC_62443/Orientierungsleitfaden_fuer_Hersteller_IEC_62443.pdf.

3ADR010839, REV C, en_US, 2021/12/14

ABB AG
Eppelheimer Straße 82
69123 Heidelberg, Germany
Phone: +49 62 21 701 1444 Fax : +49 62 21 701 1382
Mail: plc.support@de.abb.com
www.abb.com/plc