OT security for production plants with PROFINET

A classification of IEC 62443 for operators, integrators and manufacturers

Whitepaper

for PROFINET

Version 0.20 - Date February 2022

Order No.: 7.342

File name : IEC_62443_Introduction_7342_V020_Feb22

Prepared by the PROFIBUS Working Group PG10 “Security” in the Technical Committee CB.

The attention of adopters is directed to the possibility that compliance with or adoption of PI (PROFIBUS&PROFINET International) specifications may require use of an invention covered by patent rights. PI shall not be responsible for identifying patents for which a license may be required by any PI specification, or for conducting legal inquiries into the legal validity or scope of those patents that are brought to its attention. PI specifications are prospective and advisory only. Prospective users are responsible for protecting themselves against liability for infringement of patents.

NOTICE:

The information contained in this document is subject to change without notice. The material in this document details a PI specification in accordance with the license and notices set forth on this page. This document does not represent a commitment to implement any portion of this specification in any company's products.

WHILE THE INFORMATION IN THIS PUBLICATION IS BELIEVED TO BE ACCURATE, PI MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS MATERIAL INCLUDING, BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, IMPLIED WARRANTY OF MERCHANTABILITY OR WARRANTY OF FITNESS FOR PARTICULAR PURPOSE OR USE.

In no event shall PI be liable for errors contained herein or for indirect, incidental, special, consequential, reliance or cover damages, including loss of profits, revenue, data or use, incurred by any user or any third party. Compliance with this specification does not absolve manufacturers of PROFIBUS or PROFINET equipment, from the requirements of safety and regulatory agencies (TÜV, BIA, UL, CSA, etc.).

PROFIBUS® and PROFINET® logos are registered trade marks. The use is restricted to members of PROFIBUS&PROFINET International. More detailed terms for the use can be found on the web page www.profibus.com/Downloads. Please select button "Presentations & logos".

In this specification the following key words (in **bold** text) will be used:

may: indicates flexibility of choice with no implied preference.

should: indicates flexibility of choice with a strongly preferred implementation.

shall: indicates a mandatory requirement. Designers **shall** implement such mandatory requirements to ensure interoperability and to claim conformance with this specification.

Publisher:
PROFIBUS Nutzerorganisation e.V.
Haid-und-Neu-Str. 7
76131 Karlsruhe
Germany

Phone :	+49 721 986197 0
Fax:	+49 721 986197 11
E-mail:	info@profibus.com
Web site:	www.profibus.com

Table of contents

List of figures

List of tables

Version history

Version	Author	Date	Change history
0.6	Niemann	13.09.2021	First version with content
0.7	Niemann	15.09.2021	Further content added
0.9	Niemann	08.10.2021	Comments X. Schmidt edited and content completed
0.11	Niemann	10.10.2021	Glossary and index created
0.13	Niemann	12.10.2021	Version for WG Review
0.14	Niemann	01.11.2021	Comments E+H integrated and edited, Security Level assignment edited. Review comments Siemens edited
0.15	Niemann	12.12.2021	Review comments Siemens edited, safety part deleted
0.16	Niemann	16.12.2021	After WG Review. All changes incorporated. WG review completed.
0.17	Niemann	06.01.2022	Translation to English
0.18	Niemann	29.01.2022	Processing review comments of WG
0.19	Niemann	24.02.2022	Processing review comments of WG
0.20	Niemann	24.02.2022	Final formatting. Input for advisory board review

1 Management Summary - Scope of the document

Ensuring the OT security in production plants requires the interaction of various players in the OT security process. PROFIBUS & PROFINET International (PI) is one of these players. PI defines, for example, the properties of the PROFINET protocol and provides specifications for the planning and installation of PROFINET systems. Increasingly, users are asking for a classification of the PROFINET system in the OT security process and for a classification of PROFINET with respect to the requirements of relevant OT security standards, such as the IEC 62443 series.

This white paper first provides an overview of the various parts of the IEC 62443 series of standards and briefly describes their contents. This is followed by an assignment of the standard parts to the players in the OT security process. In the area of Operational Technology (OT) these are the plant operators, the system integrators and the product suppliers.

Building on these front-up considerations, a classification of PROFINET follows. The role of PROFIBUS & PROFINET International (PI) and the manufacturers of PROFINET products in the OT security process are described. The document also includes a description, how plant operators are supported in the OT security process.

2 Related documents and references

The following chapter 2.1 first lists PI documents that are related to this document and that can provide further information. Chapter 2.2 lists the cited standards and other sources.

2.1 Related documents

PROFIBUS Nutzerorganisation e. V. PROFINET IO Security Level 1 (Netload). Guideline for PROFINET. https://www.profibus.com/download/profinet-security-level-1-netload/ . Order No. 7.302, 2017.

PROFIBUS Nutzerorganisation e.V. PROFINET Security Guideline. Guideline for PROFINET. http://www.profibus.com/nc/download/specifications-standards/downloads/profinet-security-guideline/display/. Order No. 7.002, 2013.

PROFIBUS Nutzerorganisation e.V. Security Class 1 for PROFINET-Security. Guideline for PROFINET. https://www.profibus.com/download/profinet-security-guideline. Order No. 7.312, 2020.

PROFIBUS Nutzerorganisation e.V. Security Extensions for PROFINET - PI White Paper for PROFINET. https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/ . Without order no., 2019.

2.2 References / Standards

[AKE2009] Akerberg, Johan; Björkman, Mats: Exploring Network Security in PROFIsafe. In (Buth, B.; Rabe, G.; Seyfarth, T. eds.): Computer Safety, Reliability, and Security: 28thInternational Conference, SAFECOMP 2009, Hamburg, Germany, September 15-18, 2009. Proceedings. Springer, 2009; pp. 67-80.

[BSI2021] German Federal Office for Information Security (BSI): Glossary of Cyber Security. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/glossar-der-cyber-sicherheit_node.html.

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

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

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

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

[HOR2019] Horch, Alexander, Hannen, Heinrich-Theodor, Ditting, Stefan, Schween, Heiko: Verschlüsselung sicherer Kommunikation- Ein Widerspruch. In atp Magazin, 6-7, 2019; pp. 93-99.

[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.

[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.

[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_62443-2-5] IEC- International Electrotechnical Commission: IEC 62443-2-5 Implementation guidance for IACS asset owners, not released.

[IEC_62443-2-4] International Electrotechnical Commission: IEC 62443-2-4:2015+AMD1:2017 CSV Consolidated version. Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers. 2015

[IEC_62443-3-1] IEC- International Electrotechnical Commission: ISA 62443-3-1 Technical Report Security Technologies for Industrial Automation and Control Systems, Rev. 2, 2007.

[IEC_62443-3-2] 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.

[IEC_62443-3-3] International Electrotechnical Commission: IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. 2013.

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

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

[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.

[ISO_27001] International Standards Organization: ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements

[KOB2021] Kobes, Pierre: Guide Industrial Security. IEC 62443 simply explained. VDE Verlag, Berlin, 2021.

[NIE2021] Niemann, Karl-Heinz: Delimitation of the IT Security Standard Series ISO 27000 and IEC 62443 - A View on Automation Systems in the Manufacturing and Process Industry. Hannover University of Applied Sciences, Hannover, 2021.

[PNO2010] PROFIBUS Nutzerorganisation e.V. : Overview and guidance for PROFINET specifications. Technical Specification for PROFINET. Order No. 2.702. https://de.profibus.com/downloads/profinet-specification/.

[PNO2013] PROFIBUS Nutzerorganisation e.V. : PROFINET Security Guideline. Order Nr. 7.002. Nov. 2013. https://de.profibus.com/downloads/profinet-security-guideline.

[PNO2017a] PROFIBUS Nutzerorganisation e. V.: PROFINET IO Security Level 1 (Netload). Guideline for PROFINET. Order No. 7.302. 2017 https://www.profibus.com/download/profinet-security-level-1-netload/.

[PNO2017b] PROFIBUS Nutzerorganisation e. V. : Test Specification PROFINET IO Security Level 1. Technical Specification for PROFINET. https://www.profibus.com/download/profinet-security-level-1-netload/.

[PNO2018] PROFIBUS Nutzerorganisation e.V. : Security Extensions for PROFINET - PI White Paper for PROFINET. https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/, 07.09.2019.

[PNO2020] PROFIBUS Nutzerorganisation e.V. : Security Class 1 for PROFINET-Security. Guideline for PROFINET. Order No.: 7.312. 2020. https://www.profibus.com/download/profinet-security-guideline.

[PNO2021a] PROFIBUS Nutzerorganisation e.V. : Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO Version 2.4 MU3 - Oct 2021. Order No.: 2.722. https://www.profibus.com/download/profinet-specification. (Serves as draft for next release of IEC 61158-6-10)

[PNO2021b] PROFIBUS Nutzerorganisation e.V. Application Layer services for decentralized periphery. Technical Specification for PROFINET. Version 2.4 MU3 - Oct. 2021. Order No.: 2.712. https://www.profibus.com/download/profinet-specification. (Serves as draft for next release of IEC 61158-5-10).

[SAN2020] SANS Institute Glossary of Security Terms. https://www.sans.org/security-resources/glossary-of-terms/.

[VDI_2182_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA): VDI/VDE 2182 Blatt 1 Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. Beuth Verlag, Berlin, 2020.

[VDI_2182_4] VDI/VDE Gesellschaft Mess- und Automatisierungstechnik, VDI/VDE 2182 Blatt 4: Informationssicherheit in der industriellen Automatisierung Empfehlungen zur Umsetzung von Security-Eigenschaften für Komponenten, Systeme und Anlagen, 2018.

[VDM2021] VDMA - Verband der Maschinen und Anlagenbauer e. V.: Leitfaden IEC 62443 für den Maschinen- und Anlagenbau. Überarbeite Ausgabe 2021. https://www.vdmashop.de/Informatik-und-Technik/Leitfaden-IEC-62443-fuer-den-Maschinen--und-Anlagenbau---Ueberarbeitete-Ausgabe-2021---PDF-Download.html

[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 guide 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.

2.3 Disclaimer

PROFIBUS Nutzerorganisation e.V. (PROFIBUS user organization, hereinafter in this disclaimer referred to as “PNO”) has taken utmost care in the preparation of this document and compiled all information to the best of its knowledge. This document is nevertheless based on present knowledge, is of an informative character and is provided on the basis of liability exclusion. This document may be subject to change, enhancement or correction in the future without any expressive reference.

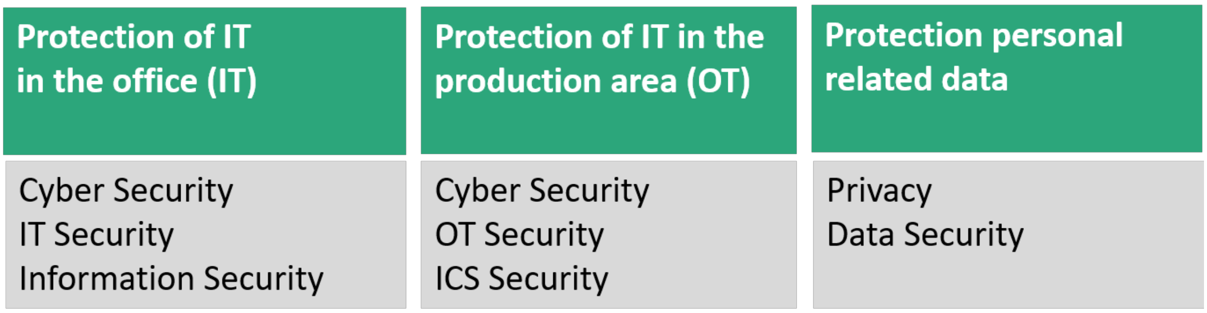
This document has no normative character. It may be useful in certain operating environments, in certain technical constellations or when used in certain countries to deviate from the given recommendations for action. In this case, the installer and operator of the installation should weigh up the advantages and disadvantages of the recommendations made in the specific application and, if deemed appropriate, decide on the implementation of a different solution if necessary.

The user may not distribute, rent or make available the Information in any other way to any third party at any time.

Any liability for defects as to quality or title of the information, especially in relation to the correctness or absence of defects or the absence of claims or third-party rights or in relation to completeness and/or fitness for purpose are excluded, except for cases involving gross negligence, willful misconduct or fraudulent concealment of a defect. Any further liability is excluded unless required by law, e.g. in cases of personal injury or death, willful misconduct, gross negligence, or in case of breach of fundamental contractual obligations.

3 Definitions and abbreviations

The following two chapters define the terms and abbreviations used. Beforehand, some terms in the field of information security are to be delineated.



Protection of IT in the office (IT)	Protection of IT in the production area (OT)	Protection personal related data
Cyber Security IT Security Information Security	Cyber Security OT Security ICS Security	Privacy Data Security

Figure 1: Delimitation of terms used

The term information security is used, as in [ISO_27001], when referring to the protection of information in general. The standard talks for example of an "information security management system". In addition to this general description, alternative terms came up in literature, such as IT security and or cyber security. The use of these terms implies that applications in a conventional IT environment and not production facilities are being considered here. Figure 1 shows the most common terms used in the field of information security. Information security in the area of production plants or comparable systems imposes additional requirements, e.g., with regard to the availability of the automation systems. To characterize this application environment with its additional requirements, terms such as OT security (OT=Operational Technology) or ICS security (ICS=Industrial Control System) are used for this purpose. The term cyber security is often used as general term and can be found in the IT as well as in the OT area. The protection of personal data, (data privacy) is not discussed in detail.

This white paper focuses on production facilities. Therefore, the term OT security is used in the following when referring to the information security of production systems. The information security of office systems is referred to as IT security.

3.1 Definitions

Table 1 shows a list of the technical terms used. The definitions of terms have been taken in part from [SAN2020] and from [IEC_62443-1-1].

Table 1: Terms used

Term	Description
Attack	Attack on a system resulting from an intelligent threat
Authentication	Authentication is the process of confirming the correctness of the claimed identity. An authentication process can involve both people and devices.
Authenticity	The term authenticity is used to describe the property that ensures that a communication partner is actually who he claims to be. Authentic information ensures that it was created by the specified source. The term is not only used when checking the identity of persons, but also for IT components or applications. [BSI2021]

Term	Description
Automation system	System for monitoring, controlling and/or regulating a technical process.
Cell protection concept	Concept for protection that provides for segmentation and mutual compartmentalization of communication systems.
Component manufacturer	In this document, the manufacturer of a component of an automation system (e.g. frequency converter), but without the role of producing an entire automation system. Distinction from the term system manufacturer. -> See system manufacturer.
Conduit	Logical grouping of communication channels to connect two or more zones that have common security requirements. -> See Zone.
Critical infrastructure	Facilities or systems that play an important role in supplying the population. Typical representatives are e.g. waterworks, power plants, sewage treatment plants above a certain size.
Cyber Security	General term for information security. Frequently used in both OT and IT.
Data security	See data protection.
Encryption	Cryptographic process that translates a plaintext into a ciphertext with the aim of making the original content inaccessible to outsiders.
Firewall	A logical or physical disruption in a network to prevent unauthorized access to data or resources.
ICS Security	See OT Security.
Information Security	The goal of information security is to protect information. The protection goals or basic values of information security are confidentiality, integrity and availability. Many users include other basic values in their considerations. [BSI2021]
Information Technology (IT)	Describes in this document information-processing systems that are not generally used to control technical processes. The term is used in distinction to Operational Technology (OT), e.g. to denote applications in the office sector. -> See also Operational Technology.
Inside Perpetrator	Attacker belonging to the organization he/she is attacking.
Integrity	Integrity refers to ensuring the correctness (integrity) of data and the correct functioning of systems. When the term integrity is applied to "data," it expresses that the data is complete and unchanged. In information technology, however, it is usually defined more broadly and applied to "information." In this context, the term "information" is used to refer to "data" that can be assigned certain attributes, such as author or time of creation, depending on the context. The loss of integrity of information can therefore mean that it has been altered without authorization, that information on the author has been falsified, or

Term	Description
	that time information on creation has been manipulated. [BSI2021]
Intrusion Detection System	A security management system for computers and networks. An IDS collects and analyzes information from different areas of a computer or network to detect possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks within the organization).
IS	See information security.
IT	See Information Technology.
IT Security	Term used in this document to describe information security for IT systems. The focus here is on the requirements of an office environment. The term is used in distinction to OT security -> See OT security. In OT security, information security requirements for production systems are considered. Since a production environment has higher requirements, a distinction is therefore made between IT security and OT security.
Maturity Level	Maturity level of an organization in terms of meeting requirements.
Office system	See Information Technology.
Operational Technology (OT),	Technology used to monitor, control and/or regulate technical processes. The term is used in distinction to Information-Technology. -> See IT
Operator,	See plant operator
OT	See Operational Technology.
OT security	Term used in this document to describe information security for technical systems, such as automation systems. The term is used in distinction to IT security. -> See IT security. Here, the focus is on the requirements of a production environment. Since a production environment has higher requirements, a distinction is made between IT security and OT security.
OT Security process	Security process for technical systems, such as automation systems.
OT security standard(s)	Standards that relate to the information security of technical systems. The IEC 62443 series of standards is relevant here.
Patch	Software package for correcting one or more errors in a software.
Plant operator	Owner of the assets of a production facility, who usually also operates that production facility.
Privacy, Data privacy	Protection of personal data.
Product supplier	See component manufacturer.

Term	Description
Production plant	Plant for the production of goods.
PROFINET system	Communication system based on the PROFINET protocol.
Risk assessment	Process that systematically identifies potential vulnerabilities to auditable system resources and threats to those resources, quantifies damage risks and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources for countermeasures to minimize the risks.
Safety system	Designation for a system that fulfills requirements related to functional safety.
Security by Design	Development process in which the aspect of information security is anchored in the development process.
Security level	Definition according to [IEC_62443-3-3]. A level of confidence that the automation system or a component thereof is free of vulnerabilities and will function in the intended manner.
System integrator	Person or company that plans and commissions production facilities or parts thereof on behalf of the plant operator.
System manufacturer	In this document: Manufacturer who can supply a complete automation system. This consists, for example, of controllers, remote IO, switches, engineering station, operating and monitoring station, etc.
Technology supplier	Person or company that supplies hardware or software components to product and system suppliers who then integrate them into their products or systems. An example of a technology supplier would be the manufacturer of a protocol stack for PROFINET.
Zone	Collection of entities that represent a partitioning of a system considering their functional, logical and physical relationship.

3.2 Abbreviations

Table 2describes the abbreviations used in the document.

Table 2: List of abbreviations

Abbreviation	Description
IT	Describes in this document information-processing systems that are not generally used to control technical processes. The term is used in distinction to operational technology (OT).
OT	Technology used to monitor, control and/or regulate technical processes. This is done in distinction to information technology, which is rather assigned to office applications.

4 Introduction to OT security for production facilities

Production plant operators are increasingly challenged to ensure the OT security of their production facilities. Spectacular attacks on critical infrastructures e.g., on an oil pipeline in the U.S.A. [CYB2020] impressively demonstrate that automation technology, the so-called operational technology (OT), is exposed to growing threats. PROFIBUS & PROFINET International (PI) addressed this aspect back in 2013 by issuing a guideline for the secure operation of PROFINET networks [PNO2013]. This guideline describes the segmentation and cell protection of PROFINET networks to ensure secure operation and protection against external attacks. However, the cell protection concept implemented in the guideline does not provide protection against internal perpetrators. It is assumed that these can overcome the perimeter protection and thus gain access to the compartmentalized network area. To provide additional protection against internal perpetrators, PROFIBUS & PROFINET International (PI) is working on an extended concept that provides for protection of communication by cryptographic checksums (cryptographic hashes), supplemented by encryption if necessary. This extended concept is described in [PNO2018]. A mapping of this concept to the PROFINET specification is also available in [PNO2021a] and [PNO2021b].

Operators of production facilities should determine the protection requirements of their facility and implement measures adapted to these protection requirements. Here, it must be determined whether the cell protection concept or extended protection by cryptographically secured protocols is required.

Information security must be assessed in a holistic approach. Both commercial data processing systems (IT) and production systems (OT) must be considered. IT and OT are to be distinguished, as shown in Table 3. PROFIBUS & PROFINET International, with its activities, is mainly focusing on OT.

Table 3: Delimitation of IT and OT

Domain	Definition according to Gartner Group [GAR2021].	Application examples
IT	Information Technology (IT) is the common term for the entire spectrum of information processing technologies, including software, hardware, communications technologies and related services. Generally, IT does not include embedded technologies as long as they do not generate data for enterprise use.	• Personal Computers • Laptops • Web Servers • Mail Servers • SAP Systems • File Servers • 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 (PLC) • Display systems (touch panels) • Server for production control • Industrial robots • Remote IO systems • Real-time networks

Although the basic requirements of IT and OT are similar in terms of information security, both application domains require differentiated approaches because, for example, in OT the aspect of availability is of high importance. Figure 2 shows the different prioritization of protection goals for IT and OT.

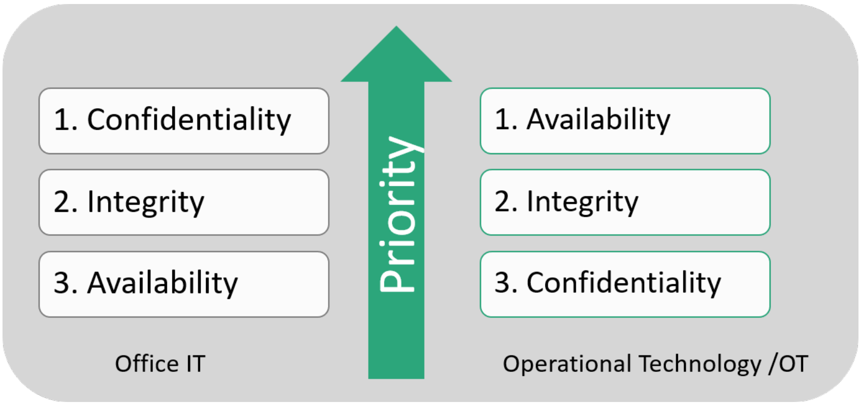


Figure 2: Protection goals IT and OT

For this reason, the ISO 27000 series of standards for the IT sector and IEC 62443 series of standards for the OT sector have been developed. Differences and similarities between these two series of standards are discussed in detail in [NIE2021].

5 The IEC 62443 standard

The IEC 62443 series of standards was developed with a focus on industrial automation technology. The standard is aimed at plant operators, integrators, and system and component manufacturers of automation systems. The concepts and procedures defined in the standard are based in many aspects on the ISO 27000 series of standards.. Figure 3 shows the parts of the IEC 62443 series of standards.

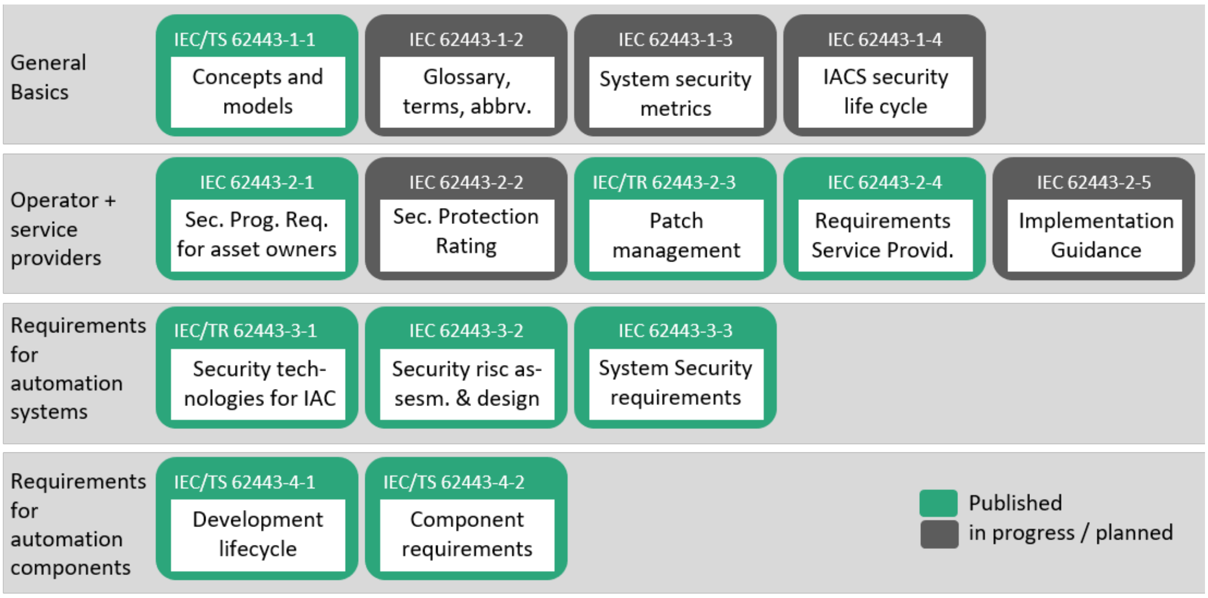


Figure 3: Structure of the IEC 62443 series of standards, based on [DKE2020]

As can be seen in Figure 3, the standard is divided into four main areas, which are described in more detail below. The parts highlighted in green have already been published. The parts with a gray background are only available as a draft for discussion and review purposes on a limited basis.

5.1 IEC 62443 - Part 1: General principles

Figure 4 shows the parts of the standard that can be assigned to the general principles.

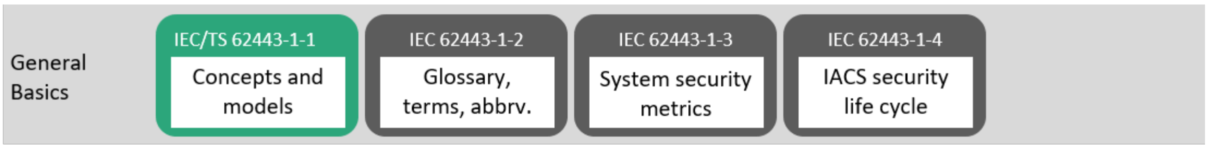


Figure 4: IEC 62443 - Part 1: General principles, based on [DKE2020]

The standard [IEC_62443-1-1] describes the basic concepts and defines the terms and security models for automation systems. The standard has the following components, among others:

- Risk analysis
- Maturity level of the security program
- Process models
- Zones and conduits
- Security models

- Reference architecture

[IEC_62443-1-2] defines the terms used in the standard. Part [IEC_62443-1-3] describes evaluation criteria (metrics) for assessing OT security. The entire security lifecycle and the associated use cases are described in part [IEC_62443-1-4]. The latter three parts are currently only available in draft form and are not yet generally accessible.

5.2 IEC 62443 - Part 2: Operators and service providers

Figure 5 shows the parts of the IEC 62443 standard that provide information for plant operators and service providers. The focus is on the security management system for plant operators and the requirements for service providers.

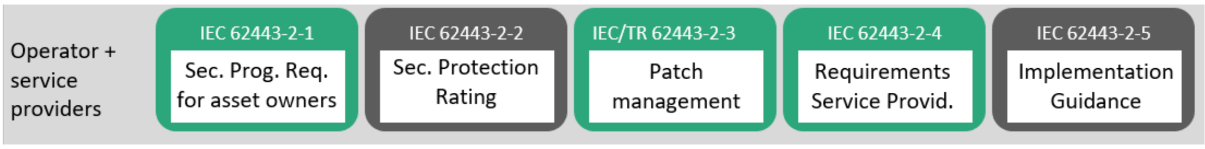


Figure 5: IEC 62443 - Part 2: Plant operators and service providers, based on [DKE2020]

The standard part [IEC_62443-2-1] defines the security management system for production plants and describes the corresponding requirements. These include, for example:

- Definition of security processes
- Risk Management
- Definition of requirements for the training of personnel
- Business continuity plans
- Access control
- Continuous improvement process
- etc.

The part [ISA_62443-2-2] first describes the roles and responsibilities in the security process, in order to realize the evaluation of the protection of an automation system by means of a holistic protection scheme. The combination of technical and organizational measures ensures the overall protection of the automation system. In the document, a corresponding evaluation scheme is presented, which enables a quantitative evaluation of the system protection via so-called protection levels. The maturity of the organization is classified via so called maturity levels. The combination of both allows a holistic evaluation of the technical and organizational requirements.

Updating the software of automation systems is a critical process, as a failed software update can potentially cause an automation system to fail. For this reason, [IEC_62443-2-3] provides comprehensive descriptions for the processing of software updates. It focuses in particular on testing and the roll out of the patches.

The use of service providers is common practice in many production facilities, e.g. for commissioning and service. The requirements for external personnel are defined in the standard part [IEC_62443-2-4]. The standard specifies procedures for external personnel, considering both maintenance service providers and system integrators.

The standard part [IEC_62443-2-5] will contain implementation instructions for operators. This part of the standard is not yet available.

5.3 IEC 62443 - Part 3: Requirements for automation systems

Figure 6 lists the standard parts that define the requirements for an automation system.

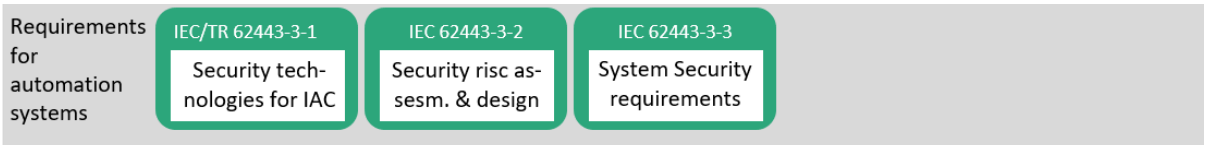

Requirements for automation systems
IEC/TR 62443-3-1
Security tech-nologies for IAC
IEC 62443-3-2
Security risc as-sesm. & design
IEC 62443-3-3
System Security requirements

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

The part [IEC_62443-3-1] describes basic security technologies, such as authentication procedures, firewalls,virtual networks, intrusion detection systems and many more. Their applicability for automation systems and any existing weaknesses are also described.

The standard part [IEC_62443-3-2] deals with the security process and in particular the security analysis of a production plant. This is then used to develop a concept for structuring the plant into zones (isolated areas) and conduits (secured connections between areas) is derived. The document then leads through the process of risk assessment in which the existing vulnerabilities, the probability of occurrence of damage and the extent of damage are compiled, evaluated and documented. Based on this risk assessment, protective measures are defined to reduce the risk.

The part [IEC_62443-3-3] defines basic requirements for automation systems. These are:

- Identification/Authentication Control (AC)
  - Capture of all users (human, software, component)
- User management (UC)
  - Enforce user access permissions
- System Integrity (DI)
  - Preventing manipulation of the IACS
- Confidentiality of data (DC)
  - Securing data in communication channels and stores
- Restriction of the data flow (RDF)
  - Zone division and protected communication channels
- Timely Response to Events (TRE)
  - Quick notification of entities about IT/OT security incidents
- Resource availability (RA)
  - Ensuring the availability of resources

Based on these basic requirements, the standard defines 99 detailed requirements for the automation system for the above-mentioned areas. Since the automation systems will be found in different areas of application, the standard distinguishes the requirements according to so-called security levels (SL) according toTable 4.

Table 4: Security level [IEC_62443-3-3]

SL	Description
SL0	No special measures, no special protection necessary
SL1	Protection against occasional or accidental infringement
SL2	Protection against a deliberate violation with simple means and low effort, general skills and low motivation.
SL3	Protection against a deliberate breach with sophisticated means and medium effort, automation skills and medium motivation
SL4	Protect against a deliberate breach with sophisticated means and significant effort, automation skills, and high motivation

Not all requirements are applicable to all security levels. Depending on the security level, more or less requirements must be met. Consequently, the plant operator can define the security level relevant to him and assign different security levels to different zones in the plant.

5.4 IEC 62443 - Part 4: Requirements for automation components

Figure 7 shows the two parts of the standard that describe the requirements for automation components and the associated development life cycle and the associated development life cycle. These two parts of the standard are relevant for the manufacturers of automation and network components.

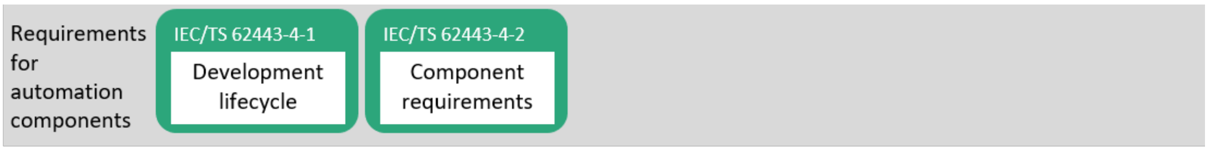


Figure 7: IEC 62443 - Part 4: Requirements for components of automation systems, based on [DKE2020]

The part [IEC_62443-4-1] deals with the secure development process for automation technology components, describes all stages of development, taking OT security requirements into account. Figure 8 shows the essential steps of the development process and the categories of the associated requirement abbreviations in the gray text fields. The aim of the concept is a security by design approach. Further information on this approach can be found in [IEC_62443-4-2] and also in [VDI_2182_4].

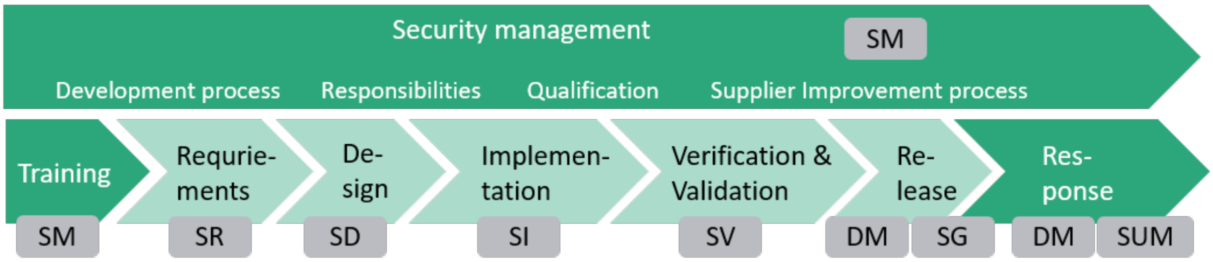


Figure 8: Secure development life cycle, based on [WAL2020]

The standard part [IEC_62443-3-3], described in the previous chapter, defines requirements for an automation system. It is understandable that the components that make up the automation system, must also meet these requirements or must support the fulfillment of these requirements. Therefore, the standard part [IEC_62443-4-2] defines requirements for components of automation systems and network components. These requirements are derived from the system requirements, but are mapped to the respective components. The standard distinguishes between component requirements (CR) and requirement enhancements (RE). These requirements are based on the system requirements (SR) defined in [IEC_62443-3-3].

The standard [IEC_62443-4-2] distinguishes between four different component types, for which requirements are defined differently in some cases.

- Software applications
- Host devices
- Embedded Systems
- Network components

The majority of the requirements apply to all component types in the same way.

5.5 Further literature on IEC 62443

Some of the standards in the IEC 62443 series are still subject to further development. Some parts of the series of standards is still in draft status. The document [ISA2020] provides an overview of the status of standardization activities. The DKE [DKE2020] provides an overview of the status of German translations.

Further information on the series of standards can be found in [KOB2021]. An overview of the IEC 62443 series of standards is given there, supplemented by the interrelationships between the parts of the standard. This book provides a compact and quick introduction to the standard. [GUN2018] provides examples for the introduction and use of IEC 62443.

In [ZVE2017], ZEVI provides component manufacturers with information on the implementation of IEC 62663 from the component manufacturer's perspective. The VDMA [VDM2021] takes the same approach with its guides for machine builders with IEC 62443.

6 The roles and responsibilities in the IEC 62443

The overview of the standard parts is aimed at different addressees as Figure 9 shows.

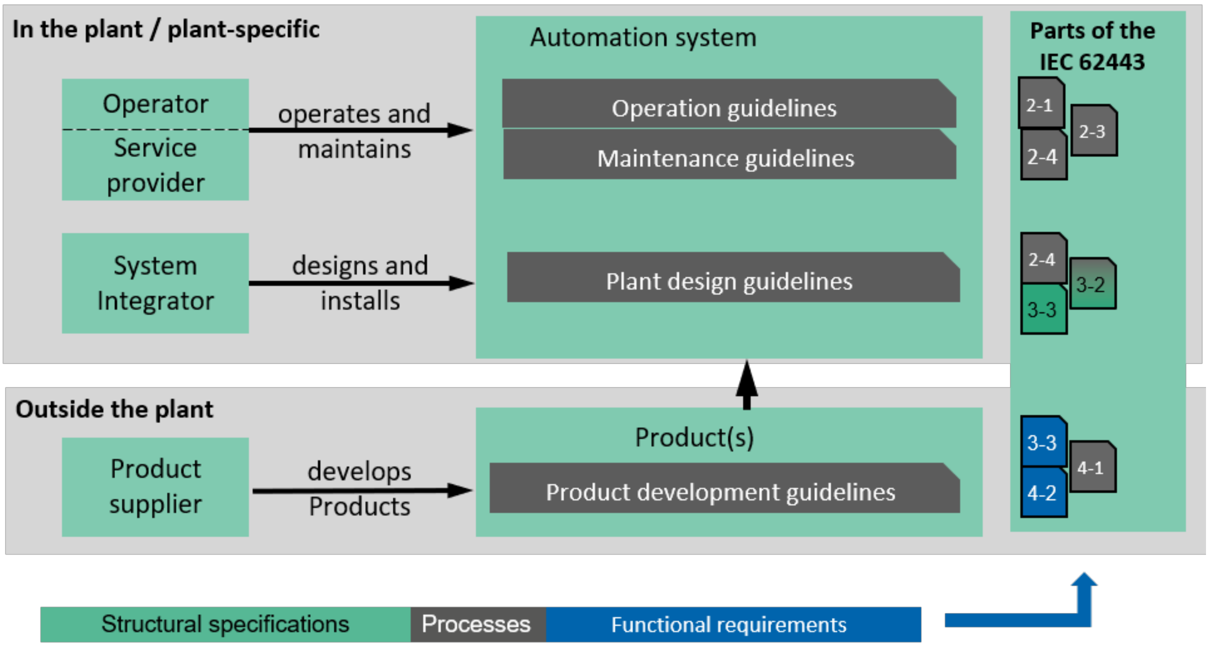


Figure 9: Assignment of roles in the security process, (based on [ISA_62443-2-2])

Essentially, a distinction is made between the roles of operator, system integrator and product supplier. The operator can also make use of service providers, e.g. for service work.

6.1 The role operator in IEC 62443

The role operator / service provider is responsible for the operation and maintenance of a production plant. For these roles, the IEC 62443 guidelines on operation and maintenance are relevant. The parts of the standard that are of interest here are the structure and operation of the Information Security Management System (ISMS) [IEC_62443-2-1] and the role of service providers [IEC_62443-2-4]. Furthermore, the part [IEC_62443-2-3] that describes the update process of the control system software (patch management), is important for the operators.

6.2 The role of system integrator in IEC 62443

The system integrator designs and installs the automation system. The part of the standard [IEC_62443-3-3] is relevant for this role. It provides specifications regarding the design and structuring of the system, e.g. in zones. The part [IEC_62443-3-2] can be used as a supplement for the security risk assessment and for the system structuring (zones). If the planning process is not carried out by the operator, but by a service provider, part [IEC_62443-2-4], which describes the requirements for service providers, must also be observed. If the plant operator carries out the planning work himself, the standards mentioned in this section also apply in similar manner to the operator in his role as plant planner.

6.3 The role of product supplier in IEC 62443

The third role to consider is that of product suppliers. For these suppliers the standard [IEC_62443-4-1] is relevant. It specifies the requirements for a secure development process (security by design). The requirements for the products that the product supplier develops are described in part [IEC_62443-4-2]. Since the requirements in this standard are derived from system requirements, the product supplier should also be familiar with these system requirements [IEC_62443-4-2] and take them into account.

7 Classification of PROFINET in the IEC 62443

PROFIBUS & PROFINET International (PI) supports its member companies in the development of products and systems. It does this by providing standards and guidelines. These standards describe the protocol itself and the use of PROFINET products in the form of application guidelines.

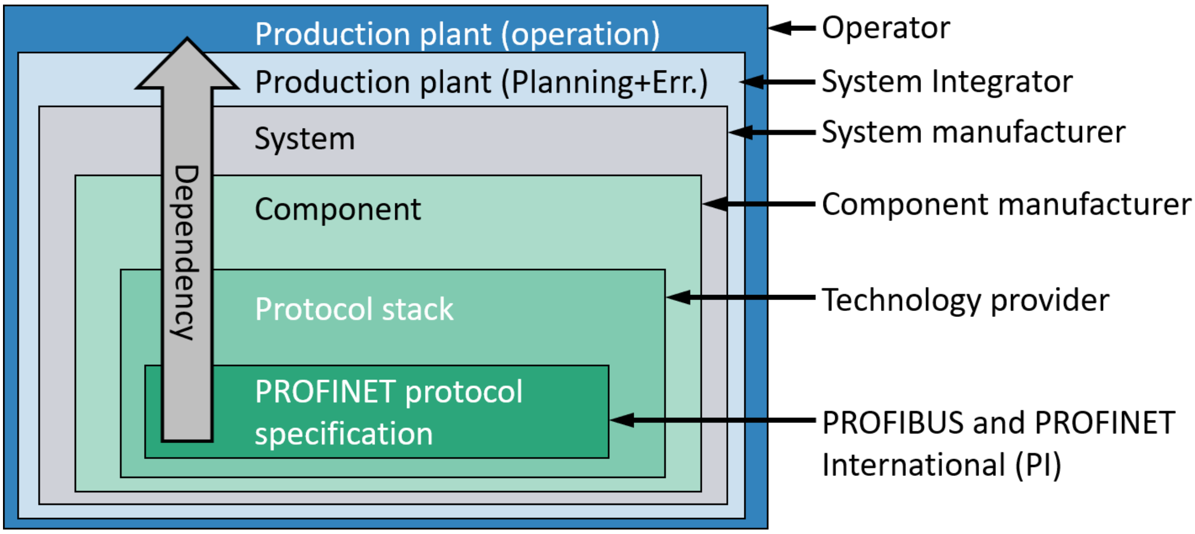

Production plant (operation)
Production plant (Planning+Err.)
System
Component
Protocol stack
PROFINET protocol specification
Dependency
Operator
System Integrator
System manufacturer
Component manufacturer
Technology provider
PROFIBUS and PROFINET International (PI)

Figure 10: The roles in the product development process

Figure 10 shows the roles in the product development process. First, PI provides protocol specifications, e.g. for PROFINET. An overview of these specifications can be found in [PNO2010]. Building on these specifications, technology suppliers then develop software components, such as PROFINET protocol stacks. Component manufacturers build PROFINET components using these software components, such as remote IO modules, frequency converters, or laser scanners. These components are assembled with other PROFINET components to form control systems. System manufacturers may have the role of a component manufacturer and technology supplier simultaneously. System integrators integrate systems and other components into production plants that are then operated by the plant operator.

The IEC 62443 series of standards defines the OT security process as a holistic process: from product development through operation to decommissioning. Therefore, many of the mentioned parties involved have to consider partial aspects of the IEC 62443 standard series in their processes. Table 5 describes the scope of delivery (deliverables) along the product creation and use process describes the respective products or services, and the role of the PI.

Table 5: Deliverables in the product development process

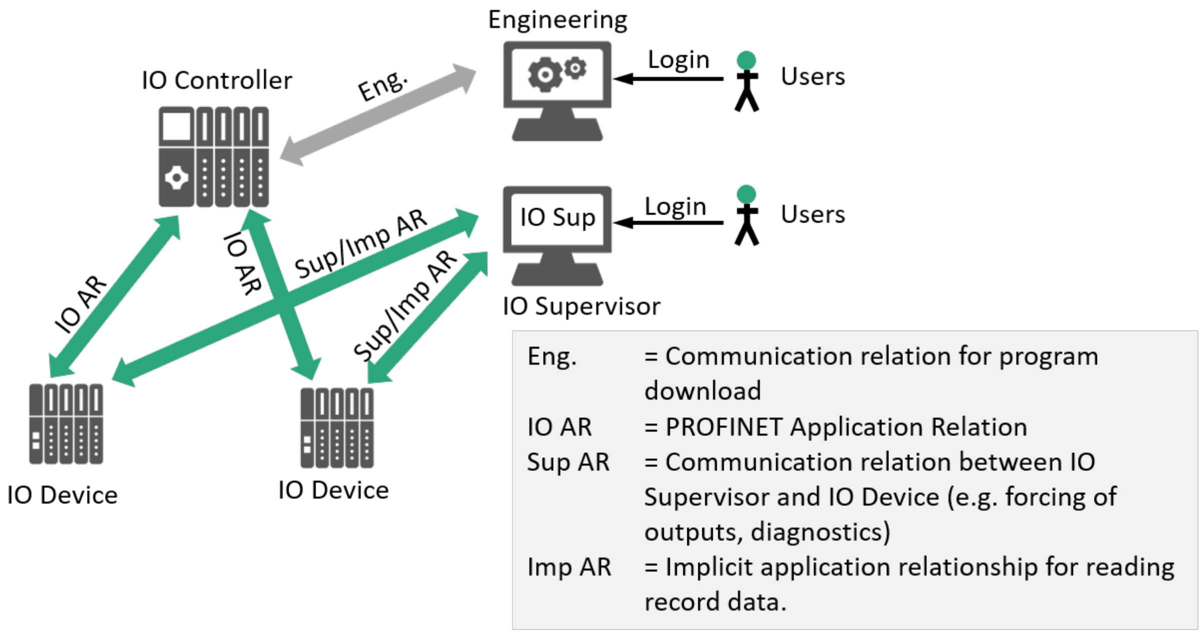
Deliverables	IEC 62443 standard part to be observed	Actor produces	PI support
PROFINET Protocol specification	[IEC_62443-4-1] [IEC_62443-4-2]	PI working group writes and evaluates PROFINET specification in compliance with the secure development process. E.g. with preceding risk analysis and observance of the functional requirements of part 4-2.	PI Working Groups (WGs) create protocol specifications taking into account the standard requirements.
PROFINET Protocol stack	[IEC_62443-4-1] [IEC_62443-4-2]	Stack supplier programs PROFINET protocol stack (software module) in compliance with the secure development process. E.g. with preceding verification of the OT security requirements by code reviews and corresponding interface and module tests and observance of the functional requirements of part 4-2.	PI working groups create. implementation notes in addition to the protocol specification to support the development process, e.g., [PNO2020].
PROFINET component	[IEC_62443-4-1] [IEC_62443-4-2]	Component manufacturer produces PROFINET component, if necessary using a protocol stack. When developing the components, the secure product development life cycle according to part 4-1 and the functional requirements according to part 4-2 must be observed.	PI working groups produce in addition to the specification: implementation notes to support the development process, e.g., [PNO2020], interpretation guide for Part 4-2 (in progress), and security test specification [PNO2017a].
PROFINET system	[IEC_62443-4-1] [IEC_62443-4-2] [IEC_62443-3-3]	System manufacturer produces control system using PROFINET components or PROFINET protocol stacks, if applicable. The secure product development life cycle according to part 4-1, the component requirements according to part 4-2 and the system requirements according to part 3-3 must be observed.	PI working groups produce in addition to the specification: implementation notes to support the development process, e.g., [PNO2020], interpretation guide for Part 4-2 (in progress), and security test specification [PNO2017a].

Production plant (planning + construction)	[IEC_62443-2-4] [IEC_62443-3-2] [IEC_62443-3-3]	System integrator plans and builds a production plant on behalf of the operator. In collaboration with the operator, he performs a risk analysis taking Part 3-2 into account and defines the required security level. He designs and structures the plant taking Part 3-3 into account and observes the requirements for service providers from Part 2-4.	PI provides description of procedures and standard solutions for PROFINET based systems considering part 3-3. See [PNO2013].
Production plant (operation)	[IEC_62443-2-1] [IEC_62443-2-3] [IEC_62443-2-4]	Operator operates plant along the life cycle from construction to decommissioning. Operator establishes and maintains OT security management process and observes the process requirements according to part 2-1. Software updates during operation are performed in compliance with part 2-3. The use of service providers takes Part 2-4 into account.	---

Table 5 shows that PI will provide supporting documentation for the individual steps of the product and plant design process. Some documents have already been published. Others are still in the process of being created.

7.1 The future OT security concept of PROFINET

PI is currently developing a security concept that uses cryptographic means to secure communication. The basic concept is described in [PNO2018]. The implementation in the PROFINET specification can be found in [PNO2021a] and [PNO2021b]. Figure 11 shows in green the communication relationships in a PROFINET system that are to be cryptographically secured in the future as part of the PROFINET specification.



Eng. = Communication relation for program download
IO AR = PROFINET Application Relation
Sup AR = Communication relation between IO Supervisor and IO Device (e.g. forcing of outputs, diagnostics)
Imp AR = Implicit application relationship for reading record data.

Figure 11: Communication relationships in the PROFINET security concept

The connection to the engineering station, which is shown in gray is also cryptographically secured. However, this protection is manufacturer-specific and is therefore not part of the PROFINET specification. User access to the engineering station and the IO supervisor must also be secured on a manufacturer-specific basis and is not part of the planned work.

The PROFINET security concept is based on the following key points:

- Protection of the communication by a cryptographic checksum (hash, Message Authentication Code)
- Depending on service additional protection through encryption
- Use of manufacturer and operator certificates to ensure the authenticity of communication participants
- Start-up of the system in a two-step process
    - Start of the connection establishment using asymmetric cryptography
    - After that transition to a symmetrical method (performance reasons)

Essential aspects of the security measures are already incorporated in the current PROFINET specification [PNO2021a], [PNO2021b].

7.2 Mapping of the PROFINET security classes to the security levels of IEC 62443

Table 4 defines the security levels specified in [IEC_62443-3-3]. The levels describe the capabilities of an attacker. The levels range from SL0 (no protection required) to SL4 (protection against attackers with high motivation and high capabilities). During the risk analysis, the operator must define the required security level for the system. Depending on the required security level, more stringent or less stringent requirements of the standard then take effect.

To meet these requirements, component manufacturers must consider the security requirements of [IEC_62443-4-2] when developing their products. The component manufacturer must specify, which security level according to Table 4 the product shall fulfill. Depending on the security level to be achieved, corresponding requirements must be met and also verified by means of a test. In addition, manufacturers must have established the secure development life cycle in accordance with [IEC_62443-4-1] when developing the products. With the PROFINET specification, PI also provides a building block for a component that considers the security requirements of [IEC_62443-4-2].

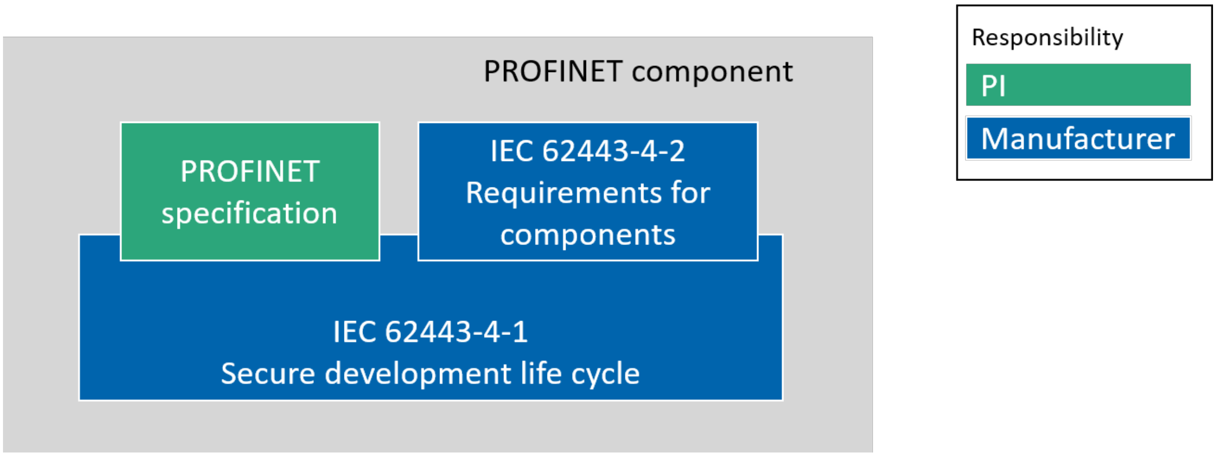

PROFINET component
PROFINET specification
IEC 62443-4-2 Requirements for components
IEC 62443-4-1 Secure development life cycle
Responsibility
PI
Manufacturer

Figure 12: Security building blocks of a PROFINET component

Figure 12 shows the building blocks of a PROFINET component with respect to security:

- PI provides the basis for secure communication of the module based on the PROFINET specification.

- The component manufacturer implements his component, whereby the communication part of the component is based on the features describe in the PROFINET specification.

- The component manufacturer develops the component in compliance with the secure product development life cycle.

It can therefore be stated that the PROFINET specification provides an important basis for a secure PROFINET component, but that the manufacturer has to consider further requirements in the product and in the product development life cycle.

In [PNO2018] PI defines the PROFINET security classes according toTable 6.

Table 6: PROFINET security classes

Security class	Name of the PROFINET security class	Definition	Typical field of application
1	Robustness	Today's state of PN security and in addition to that: SNMP default strings can be changed, DCP commands can be set to "read only", GSD files are protected against unnoticed modification by signing.	Incremental improvement to the current state of PN security.
2	Integrity + Authenticity	In addition to the requirements of security class 1, the integrity and authenticity of the assets and the communication relationships are secured via cryptographic functions. The confidentiality of the configuration data is ensured. Confidentiality of the IO data is not required.	Systems with communication relationships across plant zone boundaries. System cannot or can hardly be divided into mutually isolated zones. Access to the system cannot be secured (e.g. system outdoors without permanently present personnel). Application has no requirements regarding confidentiality of IO data.
3	Confidentiality	In addition to the requirements of security class 2, the confidentiality of all communication relationships is guaranteed.	System according to security class 2 in which company secrets can be inferred from the IO data of the system.

It can be seen that these security classes describe capabilities of the PROFINET protocol with respect to OT security requirements. A direct mapping to the security levels from [IEC_62443-3-3] in accordance with Table 4 is not possible, since the PROFINET security concept according to Figure 12 only provides one module for fulfilling the security requirements. But it is possible to decide, which component requirements of [IEC_62443-4-2] can be met by the PROFINET security classes in accordance with Table 6, provided that the remaining requirements are considered by the manufacturer.

Table 7: Assignment of PROFINET security classes to IEC 62443 security levels

IEC 62443 Security Level (SL)	Required PROFINET Security Class	Comment
SL0	any	No special requirements.
SL1	PN Security Class 2 and the consideration of the requirements of SL1 in the development of the component according to [IEC_62443-4-2].	With additional requirements in terms of confidentiality of data PN Security class 3.
SL2	PN Security Class 2 and the consideration of the requirements of SL2 in the development of the component according to [IEC_62443-4-2].	For requirements related to confidentiality of PROFINET security class 3.
SL3	PN Security Class 2 and the consideration of the requirements of SL3 in the development of the component according to [IEC_62443-4-2].	For requirements related to confidentiality of PROFINET security Class 3 and additional measures.
SL4	Currently not considered	Currently not considered

Table 7 shows that the IEC 62443 security levels SL1, SL2 and SL3 can be covered by PROFINET security classes 2 and 3, provided that the module manufacturer takes the other requirements of the respective security level into account when developing the product. Security level 4 was not considered in the previous PI analyses.

If company secrets are transferred via the PROFINET using the cyclic data (e.g. production recipes), PROFINET security class 3 should be used.

7.3 The role of PI and the manufacturers in relation to OT security

In Table 5 the deliverables of the individual players and the role of the PI were described. From this, we can derive the division of work between the manufacturers and the PI, which looks as follows.

PI: Future provision of:

1. PROFINET specification, which specifies the corresponding security features of PROFINET.
2. Documents for interpretation of the specification.
3. Extension of the PROFINET test description for testing the security features based on [PNO2017a], [PNO2017b].
4. Extension of the test system for automated testing of security functions in the test labs.
5. Software for signing of GSD(ML)-files on the basis of [PNO2020]
6. Updated PROFINET Security Guideline based on [PNO2013].

Manufacturer:

1. Implementation of a secure product development life cycle according to [IEC_62443-4-1].

2. Observation of the requirements from [IEC_62443-4-2] when integrating the PROFINET interface. The interpretation aid provided by PI (currently in progress) can be used for support. Depending on the targeted IEC 62443 security level, the manufacturer is also responsible for observing the security requirements of the respective security level when implementing and testing the product.
3. Coverage of all security aspects not covered by the PROFINET specification and affecting the component in general, e.g. user management in the engineering station or in the web server of the components, protection of communication between engineering station and automation components.

From the division of tasks, it can be seen that the PNO can supply ready-made building blocks for an OT security concept, but not for complete products or systems. This responsibility remains in the hands of the manufacturers.

7.4 What PI does not provide?

With the PROFINET protocol and the supporting documents, PI defines only a part of the automation system. The manufacturer of the component/system is responsible for ensuring the OT security of the overall system, observing the protected development life cycle according to [IEC_62443-4-1] and meeting the requirements of [IEC_62443-4-2] that are not covered by PROFINET.

7.5 Recommendation for operators with regard to IEC 62443

Operators of production facilities should position themselves as follows with regard to the OT security of their production facilities:

1. The operator is responsible for establishing and maintaining an information security management system (ISMS). This can be done either according to [IEC_62443-2-1] or according to [ISO_27001]. For the distinction between these standards and the advantages and disadvantages, see [NIE2021].
2. When planning a system, the operator or the system integrator should perform a risk analysis according to [ISA_62443-2-2] and define the required security level (SL). Alternatively, a risk analysis according to [VDI_2182_1] is possible.
3. Depending on the required security level, the result of the risk analysis and the performance of the devices (supported PN security classes), the system should be structured in accordance with [IEC_62443-3-3] and - if necessary - divided into zones. Specifications for configuration and operation should be defined in the form of a security policy.
4. The use of components developed in accordance with the requirements of [IEC_62443-4-2] can simplify the secure design of a system, but is not a mandatory requirement.
5. With regard to PROFINET systems, PI provides notes and sample configurations [PNO2013]. An update of this guideline is being planned.

The PROFINET zone concept, with the isolation of the system and subdivision into zones, represents an essential part of a defense-in-depth concept [DHS2016]. The security enhancements currently in progress, will now additionally increase the protection within a zone by cryptographically securing the PROFINET protocol.

8 Summary

This document first distinguishes between the application fields IT (classical information technology) and OT (operational technology - use in production plants) and defines the two application fields. The paper then focuses on the OT field of application. The IEC 62443 series of standards is generally used as the OT security standard. The article first provides the reader with an introduction to the OT security standard IEC 62443 and describes the parts of the standard and the secure development life cycle relevant for development.

The standard defines the roles of operator, service provider, system integrator and product supplier. The white paper describes which tasks and which parts of the standard are to be assigned to these roles.

These introductory sections are followed by a classification of PROFINET in the context of the IEC 62443 series of standards. In addition to the roles already mentioned, the roles of the PROFIBUS & PROFINET International (PI), the role of the technology suppliers, and the component and system manufacturers are introduced. The white paper then describes the respective roles to be assigned to the "deliverables" in the product development process. A basic description of the PROFINET security concept is followed by a mapping of the PROFINET security classes to the security levels of IEC 62443. The section concludes with a recommendation for operators regarding the use of the IEC 62443 series of standards.

9 Index

PROFIBUS User Organization e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 ● 76131 Karlsruhe ● Germany
Phone +49 721 986197 0 ● Fax +49 721 986197 11
E-mail info@profibus.com
www.profibus.com ● www.profinet.com