PROFINET – Future OT security requirements : What do NIS2, CER, CRA and IEC 62443 require?

Niemann Karl-Heinz, Boris Waldeck, Timon Eßlinger

Suggested citation:

Karl-Heinz, Niemann, Boris Waldeck, and Timon Eßlinger. 2025. "PROFINET – Future OT security requirements : What do NIS2, CER, CRA and IEC 62443 require?" *atp Magazin* 67 (9). https://doi.org/10.25968/opus-3768.

Abstract

Manufacturers, integrators, and operators of production systems must increasingly face regulatory requirements with regard to OT security. In addition, manufacturers are well advised to follow relevant OT security standards such as IEC 62443. It follows from the requirements described that the "security" of industrial communication must be ensured via appropriate protective measures. This article shows how the PROFINET communication protocol is currently being upgraded to meet the requirements.

atp magazin

Special print
Transforming Automation
Issue 9/2025

PROFINET – Future OT security requirements

What do NIS2, CER, CRA and IEC 62443 require?

#PROFINET Security #Cyber Resilience Act #NIS-2-Directive #CER-Directive

Manufacturers, integrators, and operators of production systems must increasingly face regulatory requirements with regard to OT security. In addition, manufacturers are well advised to follow relevant OT security standards such as IEC 62443. It follows from the requirements described that the "security" of industrial communication must be ensured via appropriate protective measures. This article shows how the PROFINET communication protocol is currently being upgraded to meet the requirements.

Karl-Heinz Niemann, Hanover University of Applied Sciences and Arts
Boris Waldeck, Phoenix Contact
Timon Eßlinger, Codewerk

▶ PEER-REVIEW: 7.8.2025

1. Requirements for future solutions

This section describes the requirements to be placed on future automation solutions. A distinction is made here between legal requirements (Chapter 1.1) and requirements from the state of the art (Chapter 1.2)

1. 1 Legal requirements

Increasing networking and digitization in industry have significantly increased security requirements. To ensure a high level of cybersecurity throughout the EU, several legal frameworks have been created by the EU, making it important that industrial communication protocols such as PROFINET improve their security measures to meet these requirements. The following sections describe the legal requirements from different perspectives of the stakeholders involved in the security process.

Operator perspective: The NIS2 Directive (Network and Information Security Directive) [1] is an EU directive that aims to ensure a high common level of cybersecurity across all member states. It defines coordinated security measures, risk management and incident reporting to improve the overall cybersecurity measures of companies based in the EU. The NIS2 Directive addresses essential and important facilities in defined sectors, such as public administration, digital infrastructure, water & wastewater, health, banking & finance, transportation, energy, service providers, post and courier, waste, chemicals, food, industry and research. It is estimated that around 30,000 companies in Germany are affected. In addition, these companies must exceed a certain size in terms of turnover and number of employees. It must be transposed into national law by the EU member states. Although implementation in Germany should have taken place by October 2024, it had not been realized by July 2025. The German implementation in the form of the NIS-2 Implementation and Cybersecurity Strengthening Act [2] was not passed by the Bundestag before the general election. Therefore, the legislative process must now be restarted. Despite the lack of implementation, operators are well advised to start implementing measures based on the NIS2 Directive.

Article 21 (1) of the NIS2 Directive [1] deals with risk management measures in the area of cybersecurity. The directive requires that appropriate and proportionate technical, operational and organizational measures are taken to manage the risks to the security of

network and information systems and to prevent or minimize the impact of security incidents on the recipients of their services and on other services. The measures referred to in the directive shall ensure a level of security for network and information systems appropriate to the risk presented, taking into account the state of the art and, where appropriate, the relevant European and international standards and the costs of implementation. In assessing the proportionality of these measures, due account shall be taken of the extent of the facilitys's risk exposure, its size and the likelihood and severity of security incidents occurring, including their social and economic impact.

Therefore, it can be seen that the NIS2 Directive focuses on the state of the art, on standards and on the proportionality of the measures. Furthermore, the NIS2 Directive also requires cybersecurity to be ensured along the supply chain. This is where manufacturers come into play.

For operators from critical sectors (e.g. energy, transport, drinking water, wastewater, etc.), the CER Directive (EU) 2022/2557 [3] also applies if they are classified as critical facilities. This directive particularly addresses resilience measures such as disaster preparedness, physical access protection, risk management measures, personal security management and awareness training.

Manufacturer perspective: The Cyber Resilience Act (CRA) [4] aims to improve cybersecurity for products with digital elements. It establishes common cybersecurity standards across the EU and obliges manufacturers to ensure the security of their products throughout their lifecycle. The CRA prescribes basic requirements for designing, developing and producing these products, as well as obligations for dealing with vulnerabilities. Figure 1 shows the basic requirements of the CRA.

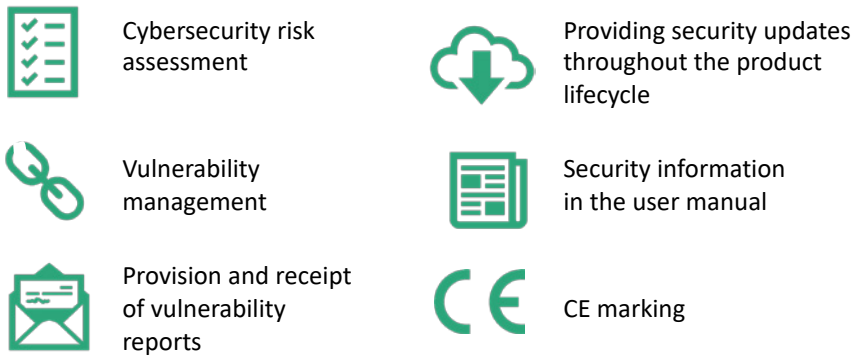


Figure 1: Basic requirements of the CRA

In contrast to the NIS2 directive, the CRA is valid without being transposed into national law. This means that:

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

From December 2027 onwards, the CRA will simplify for operators of equipment covered by the NIS2 Directive the verification of security along the supply chain.

Machine builder perspective: The EU Machinery Regulation (2023/1230) [5], hereinafter referred to as the Machinery Regulation, emphasizes the importance of cybersecurity in the design and construction of machinery. It stipulates that manufacturers must ensure that their machinery is protected against cyber threats throughout its life cycle, considering both functional safety and cybersecurity. The machine regulation also emphasizes „protection against corruption" for software and data, among other things.

1.2 Requirements from the state of the art

Although the author of article [6] questions whether standards sufficiently describe the state of the art from a legal perspective, standards will serve as the main basis for the assessment in this article. Figure 2 focuses on the manufacturer's perspective, showing the relationship between CRA and Machinery Regulation in relation to the expected standardization.

Figure 2 first illustrates that both the CRA and Machinery Regulation define OT security requirements. While the CRA focuses entirely on security, it is only a minor aspect of Machinery Regulation. The remainder considers functional safety.

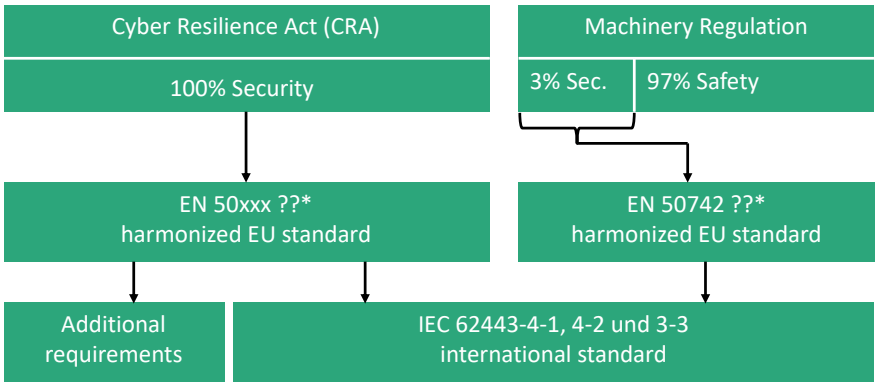
It can be assumed that harmonized European standards will be created to implement the CRA and the Machinery Regulation. These standards have not yet been adopted. The authors assume that these standards will essentially be based on the existing standards IEC 62443-3-3 [7], IEC 62443-4- 1 [8] and IEC 62443-4-2 [9].

1.3 Effects of the requirements on PROFINET security

In order to fulfill the legal requirements described, it is essential for PROFINET to meet the basic requirements in terms of integrity, authentic-

ity and, where applicable, confidentiality in the area of industrial communication. The specification work for PROFINET security was started several years ago and is available in the PROFINET specification. The latest version 2.4 MU6 [10, 11] was published in summer 2025 and replaces the version MU5.

Figure 3 summarizes the factors influencing PROFINET security. The NIS2 directive only has an indirect effect via the requirement for supply chain security. The CRA and Machinery Regulation affect with their specific requirements, both the product itself and the development life cycle. IEC 62443-4-1 affects the development life cycle, while IEC 62443-4-2 affects the product itself.



*) Standards not yet adopted

Figure 2: How do the EU Machinery Regulation and the Cyber Resilience Act fit together?

The work was essentially based on the requirements of IEC 62443-4-2 [9]. While some of the requirements are fulfilled directly by the PROFINET protocol, others that are not PROFINET-specific must be fulfilled by the manufacturers. Due to space limitations this article cannot provide a complete list of the degree of fulfillment of the requirements. PI is currently working on a corresponding document.

2. 2 Description of PROFINET security

The following chapter shows which security features PROFINET uses to technically implement the requirements defined in Chapter 1. PROFINET security is divided into classes 1 (Robustness), 2 (Integrity & Authenticity) and 3 (Confidentiality). The higher security class always includes the requirements of the lower class. Class 1 includes protection against known attacks, but no cryptographic protection of data at protocol level. Class 2 ensures the authenticity and integrity of PROFINET communication. Class 3 provides, in addition to class 2, encryption of the IO data to ensure confidentiality.

PROFINET Security does not consider the protection of communication between the controller and the engineering tool. This is manufacturer specific.

The specification of security class 1 is available in [12]. Class 2 and 3 are specified and published with the PROFINET protocol specification MU6 [10, 11] in summer 2025.

Plant operators should ask themselves which security class is required. The confidentiality of data (class 3) usually plays a subordinate role in the industrial environment. Ensuring data authenticity and integrity is much more important, for which security class 2 is sufficient. However, if confidentiality is essential, for example when transferring secret recipes, class 3 must be selected.

2.1 Security class 1

Class 1 - colloquially known as „robustness“ - offers three core functionalities that enable a gradual improvement of the existing zone protection.

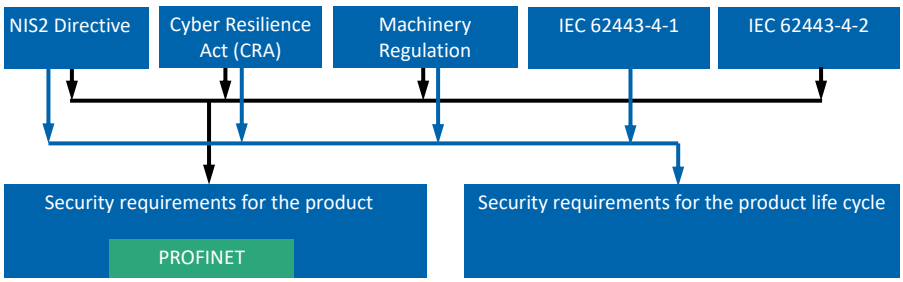


Figure 3: Factors influencing PROFINET security

1. DCP read-only mode: As soon as a PROFINET Application Relation (PNAR) has been established between the controller and the device, the DCP command can only be used for read-only access. This prevents attacks in which the IP address or the name-of-station is changed during operation via DCP to cause communication interruptions.

2. SNMP V1/V2 configuration: As the SNMP V1/V2 network protocol used by PROFINET does not offer authentication, SNMP can either be completely deactivated via class 1, set to read-only mode or the SNMP community strings can be individually enabled for read or write access.
3. GSDX: In the past, end users had no means of verifying the authenticity of a GSD file - for example, whether it originated from the specified manufacturer - or ensuring that its contents (such as IDs, parameters, etc.) had not been changed. The GSDX format extends the existing GSD with a signature from the product manufacturer. The GSD signing process is shown in Figure 4. The manufacturer can sign the GSD file and provide it as GSDX using a PI signing tool and its own manufacturer certificate. Compatible engineering tools can import GSDX files and check signatures for authenticity. The engineering tool does not need to be connected to the Internet for signature verification, as the entire certificate chain is embedded within the GSDX file. Figure 4 shows the signing process of the GSD file and verification by the user.

2.2 Security classes 2 and 3

Security class 2 ensures that attackers cannot manipulate PROFINET-IO data undetected. Class 3 offers additional encryption to prevent attackers from interpreting the data.

The core of security class 2 is the protection of the PROFINET application relation (AR) between controller and device, whereby both endpoints authenticate each other during start-up via X.509 certificates [13]. The EAP-TLS protocol is used for both security classes 2 and 3. After successful authentication, both participants negotiate a common symmetric key for the data transfer of record data, I/O data and alarms.

To maintain a high level of protection, the symmetric key is updated at regular intervals during communication.

The symmetric key is used to secure the three communication relationships shown in Figure 5. The protection of integrity and authenticity is guaranteed for all three communication relationships by means of a message authentication code (MAC). On the other hand, confidentiality is only introduced in class 3 for the I/O data. An overview of the different levels is shown in Table 1. Authenticated and authorized configuration can be used to deactivate encryption for error investigations.

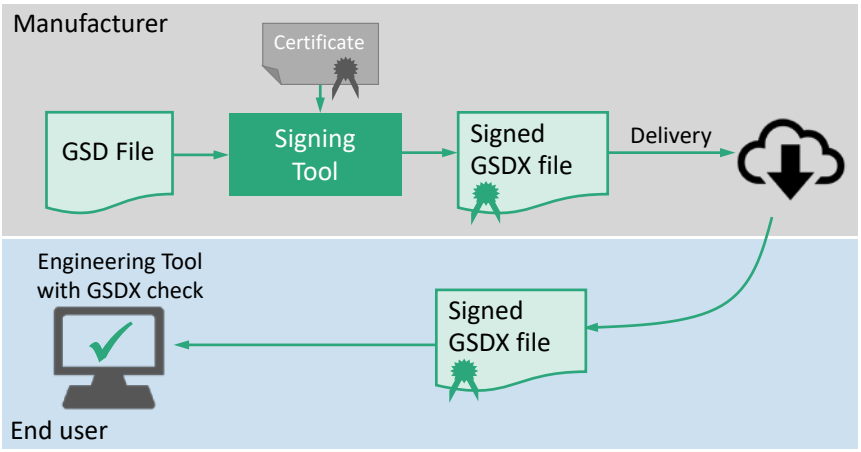


Figure 4: Signing of the GSD file and verification by the user

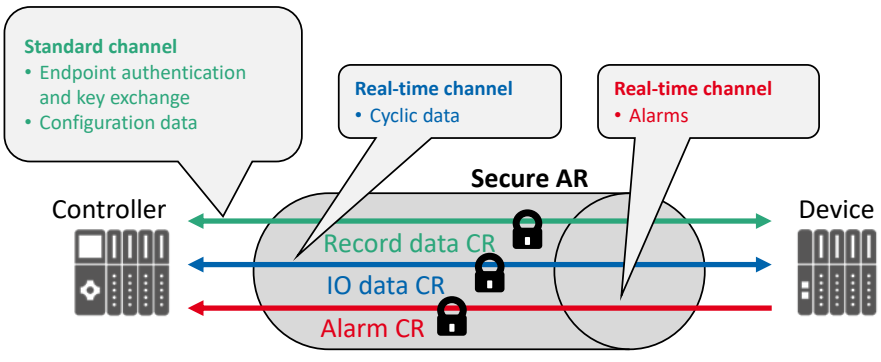


Figure 5: PROFINET Secure AR with multiple communication relationships

With security classes 2 and 3, it is also possible to granularly control communication relationships (CRs) between secure and non-secure subscribers. This allows the operator to permit mixed operation between secure and non-secure subscribers. If this is not desired, the device can be set to the state that only secure connections to the device are permitted via the so-called „security mode“ - not to be confused with the security class.

2.3 Certificate management

To ensure secure communication within a PROFINET IO system, the devices are equipped with certificates and private keys in accordance with IEEE 802.1 AR [14]. PROFINET Security considers the following X.509 certificates:

IDevID (Initial Device Identifier): This is a persistent certificate that is initially introduced into the device by the manufacturer and is managed in a TPM (Trusted Platform Module) or another secure

Table 1: Overview of security classes. Legend: (V) Mandatory, (-) Not supported (✓) Function supported, can be activated through configuration

Highest mutually supported security class (Highest security class that both communication partners can handle)	GSD-files	Record Data CR		I/O-Data CR		Alarm CR	
	Integrity, authenticity	Integrity, authenticity	Confidentiality	Integrity, authenticity	Confidentiality	Integrity, authenticity	Confidentiality
1	V	-	-	-	-	-	-
2	V	✓	-	✓	-	✓	-
3	V	✓	✓	✓	✓	✓	✓

element. The certificate is usually signed via the manufacturer's PKI. The IDevID has no direct function for PROFINET security, but it can be used to securely onboard the device with the operator.

LDevID-Generic (Local Device Identifier - Generic): This certificate is placed on the device by the system operator and forms the further basis for inserting or exchanging the LDevID-PN certificate.

LDevID-PN (Local Device Identifier - PROFINET): This certificate is application-specific and is used for mutual authentication between the PROFINET controller and device in PROFINET Security.

With the introduction of PROFINET security classes 2 and 3, the so-called PROFINET Security Configuration Management (SCM) was created. This protocol extension enables the protected handling of sensitive security-relevant data. A newly defined functional unit, the Security Infrastructure Handler (SIH), plays a central role in this process, being responsible for initiating and controlling the exchange of SCM protocols between the PROFINET components involved.

The SIH's tasks include providing, updating, removing and deactivating security configurations, certificates, keys and trust anchors. In practice, this functionality is usually integrated directly into the PROFINET controller but can also be provided by special engineering or diagnostic tools.

3. Security planning of a PROFINET system

To fulfill the requirements described in Chapter 1, generic tasks must be carried out as part of the planning in addition to the technical properties of the components used. These are described briefly below:

- Determining the parts and components that need to be considered during the security planning process.
- Identification of existing documents that have been created by the customer or system operator, such as risk assessments or the definition of the security context.
- Definition of the security context: This comprises the risk assessment and the protective measures resulting from the system's operating environment. Factors such as the location, intended use, operating conditions, external protective measures and known threats all play a role.
- Carrying out a threat and risk analysis, e.g. in accordance with IEC 62443-3-2 [15] or VDI 2182 [16]: The aim of this analysis is to identify potential hazards for the automation system or production plant. A risk analysis is prepared on the basis of the possible extent of damage and the probability of the event. If necessary, risk minimization measures are defined, and the required security level is defined in accordance with IEC 62443.
- Development of the defense-in-depth concept [17]: This concept is based on the implementation of multiple security layers to ensure a high level of protection and minimize the impact of individual security components failing. The overall security of the system is increased by combining various protective measures at different levels.
- Network planning and definition of zones and conduits: Among other things, OT security is based on the segmentation of networks in order to protect the automation network from external threats. These different network segments are defined as zones. A conduit represents a logical grouping of communication channels that fulfill security requirements for the connection between two or more zones. For an explanation of zones and conduits, see IEC 62443-1-1 [18].
- Definition of basic security features for the automation system or production plant.
- Planning of specific PROFINET security functions according to the requirements. See the following section.

- Document the results of the planning process.
- Obtain approval or sign-off from the customer or plant operator for the defined security planning.

For further details on planning, please refer to IEC 62443-2-4 [19]. The planning steps described here are useful for preparing the planning-specific steps for fulfilling the legal and normative requirements in accordance with chapter 1. The steps described are independent of the communication system used and therefore independent of PROFINET. The following section describes the PROFINET-specific planning steps.

Planning secure communication with PROFINET: PROFINET devices that use PROFINET Security are supplied with a digital certificate from the manufacturer (IDevID) and receive a second digital certificate from the system operator (LDevId). The verification of the manufacturer certificate and the provision of the system operator certificate must be planned, and the corresponding infrastructure must be in place for commissioning.

- GSDX files for PROFINET devices: PROFINET devices that support security are supplied with digitally signed GSDX files. These files are imported by the engineering tool. During the planning process, it must be ensured that digitally signed GSDX files are available.
- Planning of security relationships: The automation system to be planned usually consists of PROFINET security supported devices and may also contain devices that do not support security (legacy devices). The application relationships must be planned accordingly. All devices that support security must be configured to use a protected application relationship.
- Planning the logging of security events: Capturing and logging security-related events provides helpful information for anomaly detection and forensic investigations. PROFINET devices support the logging of events. Plans should be made to collect these events and transmit them to a security information and management system (SIEM).

PROFIBUS & PROFINET International is currently working on a „Security Planning Guideline“ to support users regarding security planning.

4. PROFINET security as an enabler for secure production

The increasing networking of industrial automation systems requires the systematic implementation of cybersecurity measures along the entire life cycle of components and systems. PROFINET Security offers a tiered security concept for this, which is based on the requirements of the IEC 62443 series and is divided into three security classes.
The regulatory requirements from the NIS2 Directive [1], the Cyber Resilience Act (CRA) [4] and the EU Machinery Regulation [5] require operators, integrators and component manufacturers to implement technical and organizational measures. The first secure solutions can already be implemented today with PROFINET security class 1 and suitable network segmentation. Specifically, these include:

- CRA
  - Integrity protection of communication
  - Partial fulfillment of the requirements of IEC 62442-4-2 insofar as they can be fulfilled by the PROFINET protocol. It is assumed that essential requirements from this standard will become part of the harmonized EU standards.
  - Security by default
  - Protection against unauthorized access
  - Confidentiality and integrity of communication
  - Minimization of data volume
  - Limitation of the attack surface
  - Recording and monitoring of security-relevant events

- NIS 2
  - Support for operators regarding supply chain security

- Machinery regulation
  - Protection of communication against intentional or unintentional corruption
  - Protection against attacks by malicious third parties

However, future requirements, particularly regarding flexible IoT structures, can only be met by implementing PROFINET security classes 2 and 3. In addition, compliance with the secure development processes defined in IEC 62443-4-1 on the side of the manufacturer contributes to supporting the security required by the NIS2 directive along the supply chain from the operator‘s point of view.

PROFINET security is a central component for safeguarding modern production systems. Secure data collection and processing is a prerequisite for compliance with regulatory requirements, as well as for the technical implementation of digitalization strategies. This includes the optimization of production processes, the integration of IT and OT systems and the reconciliation of physical and digital production levels.

To ensure the availability of compliant devices in the PROFINET security eco-

system, component manufacturers must be involved in the implementation and interoperability tests (plugfests) at an early stage. Close cooperation between all stakeholders, manufacturers, PROFIBUS & PROFINET International (PI) committees and operators creates the technical basis for secure, legally compliant and future-proof industrial automation.

IEC 62443 Security of industrial automation and control systems as a basis for PROFINET security implementation

The PROFINET specification MU 2.4 MU6 [10, 11] of PROFIBUS & PROFINET International (PI) (published in summer 2025) defines the requirements for the security of PROFINET devices, in particular for security classes 2 and 3.

IEC 62443-4-1 [8] focuses on the secure product development process at the component manufacturer and ensures that components are secure throughout their entire life cycle.

IEC 62443-4-2 [9] specifies the technical security requirements for the implementation of security classes 2 and 3 for the integrity, authenticity and confidentiality of communication for PROFINET security components.

IEC 62443-3-3 [7] describes the requirements that a system integrator must implement with regard to access, confidentiality, integrity and availability from a solution perspective. The PROFINET Design Guideline Security defines the technical implementation or additionally required organizational measures (to be published in autumn 2025).

IEC 62443-2-1 [20] defines the operator's view of security and the implementation of ISO 27001/2 ISMS security guidelines and procedures for the operation of plant and machinery.

IEC 62443-2-3 [21] explains as a technical report a set of rules for the release and installation of regular security updates and measures for software maintenance to ensure a high level of security in the long term.

IEC 62443-2-4 [19] defines the ability to safely commission and maintain systems.

These standards are supplemented by the PROFINET-specific regulations in the planning and commissioning guideline. To facilitate the implementation, conformity and interoperability of devices and systems developed in accordance with the PROFINET Security Specification, PROFIBUS & PROFINET International has published an IEC 62443 white paper [22], in which PROFINET Security is categorized in the context of IEC 62443. Figure 6 shows the interaction between the players in the security process and the associated parts of the IEC 62443 standard.

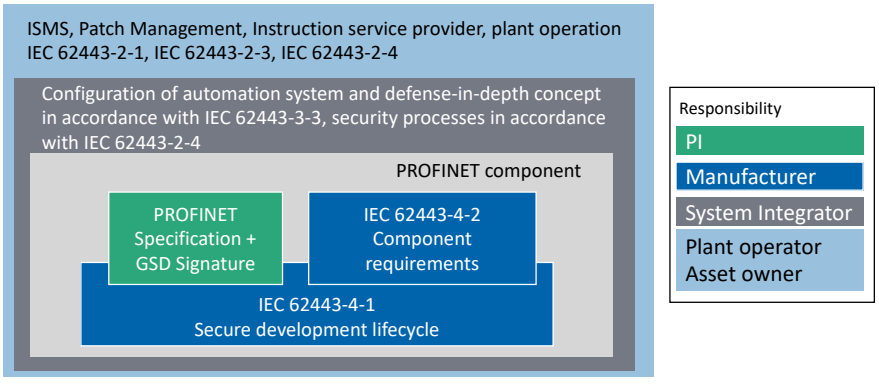


Figure 6: Responsibilities and associated parts of the standard in the security process

5. References

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

[2] Bundesministerium des Innern und für Heimat: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz). Gesetzentwurf der Bundesregierung, 2024. https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf;jsessionid=B1C0FDD365437EA35B2AF1B540EBDD15.live871?__blob=publicationFile&v=1

[3] European Parliament and of the Council of the European Union: Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. CER Directive, L 333/164-198. 2022

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

[5] Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC. In: Official Journal of the European Union, S. 1–102

[6] Seibel, M.: Abgrenzung der „allgemein anerkannten Regeln der Technik vom „Stand der Technik". Neue Juristische Wochenzeitung (NJW) (2013) 41, S. 3000–3004

[7] IEC 62443-3-3:2013:2013-06. Security for industrial automation and control systems Part 3-3: System security requirements and security levels. https://webstore.iec.ch/en/publication/7033

[8] IEC 62443-4-1:2018-01. Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. https://www.vde-verlag.de/iec-normen/249036/iec-62443-4-1-2018.html

[9] IEC 62443-4-2:2019-02. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. https://www.vde-verlag.de/iec-normen/247216/iec-62443-4-2-2019.html

[10] PROFIBUS Nutzerorganisation e.V.: Application Layer services for decentralized periphery, Technical Specification for PROFINET IO. Version 2.4 MU6 – May 2025 Nr. 2.712, 2025. https://de.profibus.com/downloads/profinet-specification/

[11] PROFIBUS Nutzerorganisation e.V.: Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO. Version 2.4 MU6 Order- Nr. 2.722, 2024. https://www.profibus.com/download/profinet-specification

[12] PROFIBUS Nutzerorganisation e.V.: Security Class 1 for PROFINET-Security Guideline for PROFINET Order No.: 7.312, 2023. https://www.profibus.com/download/profinet-security-guideline

[13] RFC 5280:2008-05. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://datatracker.ietf.org/doc/html/rfc5280

[14] IEEE 802.1AR-2018:2018. IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity. https://ieeexplore.ieee.org/document/8423794

[15] IEC 62443-3-2:2020:2020-06. Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design. https://webstore.iec.ch/en/publication/30727

[16] VDI/VDE 2182 Part 1:2020-01. IT-security for industrial automation - General model. https://www.dinmedia.de/de/technische-regel/vdi-vde-2182-blatt-1/314114388, abgerufen am: 05.05.2015

[17] Department of Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[18] IEC/TS IEC/TS 62443-1-1:2009:2009-07. Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models. https://webstore.iec.ch/publication/7029, abgerufen am: 10.05.2015

[19] IEC 62443-2-4:2023:2023-12. Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers. Ed. 2.0. https://webstore.iec.ch/en/publication/67631

[20] IEC 62443-2-1:2024:2024-08. Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners. https://www.vde-verlag.de/iec-normen/254227/iec-62443-2-1-2024.html

[21] IEC TR 62443-2-3:2015:2015-07. Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment. https://webstore.iec.ch/en/publication/22811

[22] PROFIBUS Nutzerorganisation e.V.: OT security for production plants with PROFINET. A classification of IEC 62443 for operators, integrators and manufacturers Nr. 7.342, 2022. https://www.profibus.com/download/white-paper-ot-security-classification-of-iec62443

Autoren

Prof. Dr.-Ing. Karl-Heinz Niemann (born 1959) has represented the Process Informatics and Automation Technology department at Hannover University of Applied Sciences and Arts (HsH) since 2005. Since the beginning of 2023, he has been Director of the Institute for Sensor Technology and Automation at HsH. From 2002 to 2005, he was responsible for process data processing at the University of Applied Sciences and Arts Northeast Lower Saxony (now Leuphana University). Prior to this, he held leading positions in the development of process control systems at ABB, Elsag Bailey and Hartmann & Braun. He heads the CB/PG3 - Installation Guides working group at PROFIBUS & PROFINET International and is a member of the CB/PG10 - Security working group.

Prof. Dr.-Ing. Karl-Heinz Niemann
Hanover University of Applied Sciences and Arts,
Faculty I - Electrical Engineering and Information Technology,
P.O. Box 92 02 61, D-30441 Hanover,
Phone +49 511 92 96 12 64,
E-Mail: Karl-Heinz.Niemann@HS-Hannover.de
Websites: https://hs-h.de/isa ;
https://orcid.org/0000-0001-8931-6789

Timon Eßlinger, M.Sc. (born 1994), heads the IT and OT security team at Codewerk GmbH. He specializes in securing industrial components and critical infrastructures in the context of IEC 62443, from requirements to secure development and penetration testing. He is a member of the PI CB/PG10 Security working groups at PROFIBUS & PROFINET International and in AK 351.0.6A IT Security in Railway Systems at the German Electrotechnical Commission (DKE).

Timon Eßlinger, M.Sc.
Codewerk GmbH
Östliche Rheinbrückenstr.50 | BK 148
76187 Karlsruhe
E-Mail: timon.esslinger@codewerk.de
Website: https://www.codewerk.de/

Dipl.-Ing. Boris Waldeck (born 1963) is Master Specialist Security PLCnext Technology and Product Solution Security Expert (PSSE) at Phoenix Contact GmbH & Co. KG in Bad Pyrmont. He is responsible for the IEC 62443-4-1 Secure Development life cycle (SDL) certification of the Automation Systems BU and the IEC 62443-4-2 product certification of PLCnext Control. As PSSE he supports the introduction of the SDL and product certifications according to IEC 62443 with regard to the upcoming legal regulations CRA and NIS2 in the EU. He is a member of the PI CB/PG10 Security working group at PROFIBUS & PROFINET International and the Industrial Security working group of the VDMA.

Dipl.-Ing. Boris Waldeck
PHOENIX CONTACT GmbH & Co. KG
Dringenauer Str. 30
31812 Bad Pyrmont
E-Mail: bwaldeck@phoenixcontact.com
Website: https://www.phoenixcontact.com,
https://phoe.co/Cyber-Security