atp magazin

Specialprint

Transforming Automation
Issue 9/2023

Peer-Review: 21.06.2023

How to develop a secure PROFINET device

Organizational and technical OT security measures during the development of PROFINET devices

Karl-Heinz Niemann, Hanover University of Applied Sciences and Arts; Andreas Walz, Offenburg University of Applied Sciences;
Simon Merklin, Endress+Hauser Digital Solutions; Dominik Ziegler, Siemens Aktiengesellschaft Oesterreich;
Boris Waldeck, Phoenix Contact Electronics

The PROFINET protocol has been extended in the current version [1] [2] to include security functions. This allows flexible network architectures with the consideration of OT security requirements to be designed for PROFINET, which were not possible due to the network segmentation previously required. In addition to the manufacturers of the protocol stacks, component manufacturers are also required to provide a secure implementation in their devices. The necessary measures go beyond the use of a secure protocol stack. Using the example of an Ethernet-APL transmitter with PROFINET communication, this article shows which technical and organizational conditions will have to be considered by PROFINET device manufacturers in the future.

PROFINET security / Secure development lifecycle / IEC 62443

1. Description of the current situation

With version 2.4MU4 of the PROFINET specification [1, 2], PROFIBUS & PROFINET International (PI) provides OT security functions for PROFINET. These functions serve as a basis for manufacturers of automation components and automation systems to develop components and systems that meet high standards in terms of OT security. The PROFINET security concept is based on cryptographic protection of PROFINET communication and other measures. Key features of the PROFINET security concept are:

- Equipping PROFINET devices and PROFINET controllers with digital identities via digital certificates.
- Secure establishment of application relations using the EAP-TLS protocol (asymmetric cryptography).
- Secure PROFINET communication, especially for the real-time channel, using symmetric cryptography.
- Protection of the device description files and resources (GSD files) by a digital signature.

A more detailed description of the PROFINET security concept can be found, for example, in [3 to 6].

With the specification of the PROFNET security concept, manufacturers of automation components are now faced with the challenge of integrating these security functions into their devices. The following article describes the essential tasks and processes from a manufacturer‘s point of view, using an Ethernet-APL field devices operated in conjunction with the PROFINET protocol as example.

In this document, the term „security“ is used in the sense of OT security. It, therefore, describes the protection of production facilities against cyber-attacks.

2. The role of a field device manufacturer in the security process

Field device manufacturers are currently facing several challenges. In the past, field devices were mainly equipped with a 4 ... 20 mA interface with HART protocol or via a fieldbus, such as PROFIBUS-PA. In the future, the existing interface portfolios will be supplemented or replaced, e.g., by an Ethernet-APL interface. Ethernet-APL is a two-wire Ethernet that supplies field devices with both data and power. With this interface, the field devices become PROFINET devices if using PROFINET and must meet all the requirements relevant for PROFINET devices. This also applies to the security aspect. In [7], the authors describe which security requirements are relevant for an Ethernet-APL field device.

A description of the various roles in the OT security process will now follow.

Figure 1 shows that technical and organizational requirements are relevant for the field device manufacturer as part of field device development. If these are met, the field device manufacturer can bring a secure field device to the market. Such devices are used to set up a production plant. The plant designer (system integrator) must take technical and organizational

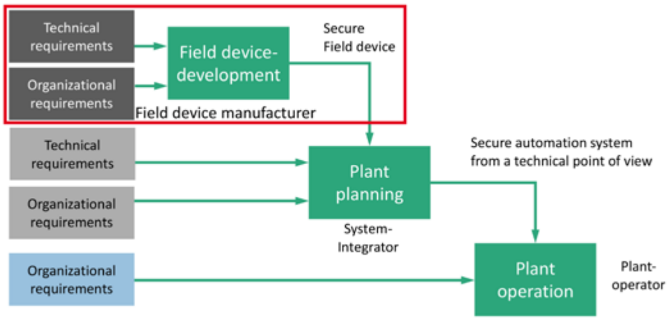
Technical requirements
Organizational requirements
Field device-development
Secure Field device
Field device manufacturer
Technical requirements
Organizational requirements
Plant planning
System-Integrator
Secure automation system from a technical point of view
Organizational requirements
Plant operation
Plant-operator

Figure 1: The roles in the OT security process

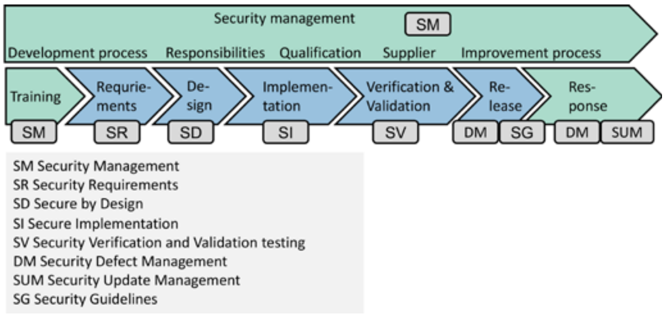

Figure 2: The components of the secure development life cycle

requirements into account during the planning process. The secure field devices are included in the planning process because they build the basis for meeting the system-wide security requirements. The system planned by the system integrator is then built, commissioned, and handed over to the operator. The system operator must observe organizational requirements relating to system operation. A detailed description of the roles described here and the assigned tasks can be found in [8].

In the following, the process shown in Figure 1 will be further detailed with a focus on a field device manufacturer. The following chapters therefore focus on field device development and show which organizational and technical requirements must be observed by the field device manufacturer to deliver a secure field device to the market at the end of development.

3. The development of a secure field device

The OT security requirements for field devices have already been discussed in previous articles [9, 10]. For this reason, the determination of the security requirements will not be discussed in detail here. Instead, this paper focuses on the development process for developing a secure field device and the required process steps.

The IEC 62443 standard has established itself as the essential standard for OT security. An overview of IEC 62443 can be found in [11]. IEC 62443 defines the role of the component manufacturer, among other things. See also the role description in Figure 1. The following two parts of the standard are relevant for the field device manufacturer role:

- » IEC 62443-4-1 [12]: This part deals with the secure development life cycle for automation components. The organizational requirements are therefore essentially found here.
- » IEC 62443-4-2 [13]: This part describes the technical requirements to be met by the components.

The following two chapters will now deal in detail with the requirements of these two standards.

3.1 Organizational requirements for the secure development life cycle

IEC 62443-4-1 describes the requirements that a development organization must fulfill to develop products that meet security requirements. This is based on a standardized development process, the secure development lifecycle (SDL). Figure 2 shows the essential components of the SDL. The goal of the SDL is to ensure that OT security requirements are considered throughout the entire lifecycle of the product and that the implementation is of consistent quality with respect to the OT security requirements. These components of the SDL are considered in more detail below.

3.1.1 Management of the security life cycle (Security Management)

This part describes how the management of the SDL will be done. The development process is defined, implemented, and reviewed, responsibilities are defined and assigned. The required qualification of personnel has been defined and is maintained and improved through continuous training. Requirements for supplier parts (e.g., protocol stacks) have been defined and are monitored. The aim here is to ensure that security requirements are also considered for supplier parts and that manufacturer notifications of vulnerabilities are also available. The security of the development environment is ensured and monitored. This is for example relevant for the integrity protection of important files, the protection and secure storage of private keys, and the monitoring of the security properties of externally provided components, such as protocol stacks. The organization must be able to handle its security-related issues, e.g., by receiving vulnerability reports from customers or other organizations and handling them according to a defined process. The described process must be regularly verified and continuously improved.

3.1.2 Security Requirements

This section of the standard deals with the processes for handling security requirements. First, the security context of the product is described. This description is necessary to define which security properties the product‘s environment provides and which requirements the product itself must fulfill.

The next step is to create a threat analysis that records and evaluates all threats affecting the component. In the case of field devices, the communication interfaces (e.g., PROFINET interface, OPC UA interface, Bluetooth interface, local display) must be considered. A detailed threat and risk analysis for a field device can be found in [10]. Based on these requirements, the IT security requirements for the component and the IT security requirements for the environment in which the component is operated are now specified. These security requirements should preferably be documented in a requirements management tool and tracked throughout the product development life cycle.

3.1.3 Secure design

This part of the standard deals with the secure design. In this regard, the standard [12] states: „*A process shall be employed to identify and manage the security risks of all externally provided components used within the product.*“ Furthermore, this part of the standard describes the Defense-in-Depth concept for the component. This concept describes the combination of component-related protective measures in conjunction with external measures. Further information on the topic of Defense-in-Depth can be found in [14 to 16].

The system/software design must then be subjected to a design review. Best practices of secure design, such as attack surface reduction, minimum privilege method and documentation of all trust boundaries, shall be used.

3.1.4 Secure implementation

The standard [12] writes on this topic: „*A process shall be employed to ensure that implementation reviews are performed for identifying, characterizing and tracking to closure security-related issues associated with the implementation of the secure design.*“ Possible review processes include the definition and the monitoring of coding rules especially related to IT security, static code analysis, flagging of IT security requirements in code, validating inputs that exceed trust limits, etc.

3.1.5 Verification and validation

This section deals with the verification of IT security requirements. This includes, for example, functional tests, performance tests [17] as well as limit and boundary condition tests. The tests should be based on generally accepted test concepts, such as those described in [18 to 20].

When designing the tests, special focus should be placed on finding security vulnerabilities. This should include fuzzing and penetration testing. The testers should act independently of the development.

3.1.6 Treatment of security-related issues

The company must be able to receive and process reports relating to vulnerabilities or defects in its own products. This also applies to vulnerability reports of third-party components (e.g., protocol stacks, operating systems). This can be done, for example, via a special e-mail account or via a website. A process must be established to ensure systematic and timely processing of such reports. For this purpose, the manufacturer can, for example, set up a Product Security and Incidence Response Team (PSIRT). The result of the processing should be communicated to the reporting person. Furthermore, if a vulnerability exists, information should be issued to the users (security bulletin, security advisory). Separate standards exist for vulnerability management and for the disclosure of vulnerabilities [21, 22].

3.1.7 Security Update Management

Due to a defect report, it may be necessary to update the product‘s software via a security patch. A process must be established that enables the creation of such updates. The security patches shall be documented and provided independently of other updates. Field devices often use dependent components, such as real-time operating systems and/or protocol stacks. Such components are to be monitored with regard to the reporting of vulnerabilities and, if necessary, required updates are also to be generated for the own product.

Users of the software updates must be able to verify the authenticity of the updates. This can be done, for example, by digitally signing the software packages.

3.1.8 Security Guidelines

The manufacturer must provide the user with security-relevant information. This includes:

- Documentation of the underlying Defense-in-Depth concept.
- Features related to the Defense-in-Depth concept that are expected from the environment.
- Component hardening policies, such as turning off unneeded services and the mandatory change of default passwords.
- Guidelines for secure disposal, e.g., deletion of digital certificates.
- Policies for secure operation, such as actions that users or administrators must perform.
- User account management policies.

The documentation shall be reviewed at regular intervals for consistency, completeness, and correctness.

3.2 Applicability and implementation of the organizational requirements to an Ethernet-APL transmitter.

The information provided in the preceding section 3.1 represent the organizational basis for the development of secure products. These organizational requirements exist regardless of the size or complexity of the device under consideration. Suppliers of Ethernet-APL transmitters should consequently address these requirements and integrate them into the development lifecycle.

For the implementation of the requirements, a step-by-step approach with the following steps may be useful:

1. Create a training plan and start security training for the staff. This training should be adapted to the roles of the employees (e.g., SW developer, SW architect, SW tester).

2. Document the development lifecycle and create the necessary documents and templates.

3. Establish the infrastructure, such as a website, for the publication of security advisories, as well as a point of contact for receiving vulnerability reports.

4. Establish the infrastructure for generating and issuing security patches, including a reporting system to customers.

5. Establish the processes for security monitoring of dependent components (e.g., operating systems, protocol stacks). Planning of security supplier audits.

6. Integrate the security-related work packages into the existing development lifecycle and the training plans of the employees.

7. Select a component for a first run through of the processes. Preferably, this should be a new component to be developed, so that all essential steps of the development life cycle are conducted. In the case of an existing component, a corresponding post-documentation effort is to be expected, even though the product is already on the market.

8. Define requirements:

   a. Develop and document the Defense-in-Depth concept.

   b. Create the threat and risk analysis.

   c. Derive the security requirements from the threat and risk analysis.

   d. Derive the security requirements from the IEC 42443-4-2 standard [13], which defines the security requirements for a component.

   e. Integrate the security requirements into the requirements management, preferably via an appropriate tool.

9. Implementation:

   a. Monitor secure design.

   b. Conduct design reviews.

   c. Perform code reviews.

   d. Perform vulnerability analyses.

10. Verification and testing:

   a. Test of the security functionality.

   b. Perform penetration testing.

   c. Perform vulnerability tests.

   d. Perform load tests. See also [17].

11. Documentation:

   a. Document the Defense-in-Depth concept.

   b. Document the requirements for environment in the context of the Defense-in-Depth concept.

   c. Document the hardening of the component.

12. Release.

The following aspects must be considered when establishing these processes:

» Documentation of the process.

» Guiding question: Where is written that you do this?

» Documentation of process results (e.g., threat and risk analysis, Defense-in-Depth concept.

» Guiding question: Do all required artifacts exist for the developed product, such as specifications, code review protocols, test documentation?

» Evidence that the processes were applied in the development of the product.

» Guiding question: Have all required documents been created for this software version and have all security requirements been implemented and tested?

» Continuous improvement of the process.

» Guiding question: What improvements have you made since the last run?

The authors advocate to first introduce the secure development lifecycle, when starting the development of a secure product. The IEC 62443-4-1 standard [12] differentiates four maturity levels. The maturity levels ML1 to ML4 describe how stable and established the security processes are within the company.

» Maturity level ML1 describes that processes in the company are partially undocumented and may not be traceable.

» Maturity Level ML2, the manufacturer has "the capability to manage the development of a product according to written policies (including objectives). The product supplier also has evidence to show that personnel who will perform the process have the expertise, are trained and/or follow written procedures to perform it."

Table 1: Definition of the security levels [13]

Security level	Description
1	Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
2	Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
3	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
4	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

- Maturity level ML3: "The performance of a manufacturer with maturity level 3 is demonstrably repeatable within the manufacturer organization. The processes have been performed and there is verifiable evidence to support them."

- Maturity level ML4, on the other hand, defines strongly controlled and continuously improved processes.

In a subsequent step, the product requirements should then be processed according to IEC 62442-4-2 [13].

3.3 Technical security requirements for an Ethernet-APL transmitter

After the organizational requirements for a development organization have been described in the previous section, the technical requirements are now considered. Before discussing the requirements in detail, two classifications must first be made: The target security level to be achieved and the type of device.

The security level describes the capabilities of an attacker, as shown in Table 1 .

Table 1 shows that the assumed capabilities of the attacker increase as the security level increases. To define the security requirements, it is first necessary to define the target security level (i.e., the level that you would like to achieve with your product). It is understandable that the requirements of the standard increase as the security level increases. The standard additionally defines requirement enhancements (RE) for higher security levels, which must be met. The targeted security level must be considered accordingly in the threat analysis. For automation systems with typical requirements, the VDMA assumes a security level of 2 in a guideline [23].

Furthermore, IEC 62443-4-2 [13] distinguishes between different component types, some of which must meet different requirements. The following component types are defined:

- Software Applications (SAR);

- Embedded Devices (EDR);

- Host devices (HDR); and

- Network Components (NDR).

An Ethernet-APL transmitter is to be classified in the category "Embedded Device (EDR)". With these two definitions, the component requirements of the standard can then be considered in a next step. The IEC 62443-4-2 standard [13] defines the following groups of requirements (Foundational Requirements):

- Identification and authentication control (IAC),

- Use control (UC),

- System integrity (SI),

- Data confidentiality (DC),

- Restricted data flow (RDF),

- Timely response to events (TRE), and

- Resource availability (RA).

In the following, the application of these requirements to the device will be discussed using an exemplary Ethernet-APL transmitter.

Figure 3 shows an exemplary Ethernet-APL transmitter. A large number of interfaces is assumed for this analysis. Real transmitters will typically have fewer interfaces. Mainly the transmitter's interfaces to the outside are to be considered, because potential attackers most likely gain access to the device via these paths.

3.3.1 Identification and authentication control

This part of the standard specifies that human users, interacting with the device, must be identified and authenticated. In the present use case, these would be, for example, human users interacting with the device via a web server or wireless on-site communication. These requirements go beyond the PROFINET security concept because other interfaces, in addition to the PROFINET interface, must be considered here. The same applies to software processes and other components. For example, an OPC UA client that accesses the OPC UA server of the device would also have to authenticate itself. This function can be performed by user account management, but also by digital certificates from a public key infrastructure (PKI certificates). The use of the display for entering configuration data must also be considered.

3.3.2 Usage control

This requirement group is related to the requirements from the previous chapter. It is required that the components also enforce the required authorization and that inactive sessions (e.g., web server access by browsers) are automatically closed. This also applies to remote service connections. To prevent excessive resource consumption and possible associated malfunction due to many parallel connections, the number of parallel connections should be limited. For example, you could specify that the transmitter only accepts one connection from the web server and rejects further connection attempts. The transmitter must log security-relevant events with a time stamp and save them persistently for analysis purposes and/or report them to a higher-level system.

3.3.3 System integrity

According to the IEC 62443, "system integrity" includes "data communication integrity". This means that the communication links are integrity-protected. This is where the PROFINET security concept comes into play. By using a PROFINET protocol stack with corresponding security function, this requirement can be met for the PROFINET interface. The same applies to the OPC UA interface and the web server interface. Secure protocol variants are available here in all cases. The interfaces must perform validation for incoming data. For example, overlong or incorrectly formatted data packets that may be deliberately used for an attack, should be detected and rejected. The transmitter must not provide any usable feedback information to a potential attacker.

The integrity of sessions is to be guaranteed by individually generated session identifiers that are to be discarded at the end of the session. This is intended to prevent so-called replay attacks, for example. This requirement is also guaranteed by the PROFINET security concept.

The integrity of the boot process must also be ensured according to the standard.

3.3.4 Data confidentiality

In contrast to IT security, confidentiality is less of a concern for process data. Nevertheless, this topic is addressed in the standard with respect to the protection of data stored in repositories for which a read authorization is required. Furthermore, the standard requires that the component "*uses cryptographic security mechanisms in accordance with generally accepted IT security practices and recommendations in information technology*" [13].

The PROFINET security concept addresses the issue of confidentiality in the form of three different security classes.

Table 2 shows the three security classes for PROFINET. Security class 1 introduces integrity protection for GSD files. Class 2 provides integrity and confidentiality protection for record data services and integrity protection for real-time communication. Class 3 then provides complementary confidentiality protection for real-time communication. This gradation was chosen because protecting confidentiality through encryption is computing time intensive and because it is assumed that there is little need for confidentiality protection for real-time data. It is therefore assumed that mainly security class 2 functions will be used in many applications.

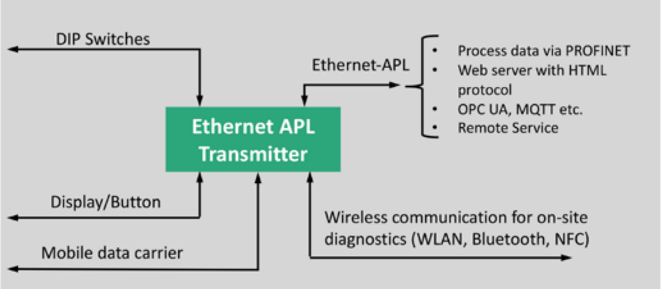
DIP Switches
Ethernet-APL
Process data via PROFINET
Web server with HTML protocol
OPC UA, MQTT etc.
Remote Service
Ethernet APL Transmitter
Display/Button
Wireless communication for on-site diagnostics (WLAN, Bluetooth, NFC)
Mobile data carrier

Figure 3: Exemplary Ethernet-APL transmitter with interfaces

3.3.5 Restricted data flow

This group of requirements is essentially concerned with the compartmentalization concept of a production plant and the division of a plant into different security zones. This aspect is not considered further in this publication, as it is not relevant for an Ethernet-APL transmitter.

3.3.6 Timely response to events

This aspect of the standard considers the collection, provision of event logs and access to these logs. To create these logs, continuous monitoring of the components must be implemented to be able to detect and log security breaches.

3.3.7 Resource availability

This section of the standard is devoted to protection against denial-of-service attacks, among other things. This addresses attacks that aim to compromise the availability of a resource, e.g., by flooding the device with requests. To meet this requirement, devices must protect their resources (e.g., computing power and memory) against overload. This is done firstly by taking appropriate precautions in the protocol stack (discarding data packets in the event of overload) and secondly by limiting the number of parallel connections, for example. In addition, a specified load resiliance for PROFINET devices is required in [17].

The aspects of data backup, system recovery and emergency power supply are not relevant for Ethernet-APL transmitters. Furthermore, the component must support the configuration of the network and security settings. It is therefore expected that services that are not required (e.g.. web server) can be deactivated or have been already deactivated in the delivery state. The aim is to operate the device with the functionality that is currently required (least functionality) and to deactivate services that are not required, as these could be potential entry points for attackers.

The creation of an asset inventory (list of all components of a plant with their hardware and software version) is a fundamental measure in OT security. The components are expected to support the creation of such an inventory with an appropriate interface.

Table 2: Security classes for PROFINET

Highest mutually supported security class	GSD files	Record Data Services		Real-time communication	
	Integrity and authenticity protection	Integrity and authenticity protection	Confidentiality	Integrity protection	Confidentiality
1	V	–	–	–	–
2	V	√	√	√	–
3	V	√	√	√	√
(V: mandatory, -: not supported, √: enabled by default)					

3.4 Applicability and implementation of the technical requirements to an Ethernet-APL transmitter.

The listing of the various requirements in section 3.3 has shown three classes of requirements from IEC-62443-4-2:

1. Requirement is not relevant for an Ethernet-APL transmitter: E.g. emergency power supply, zone boundary protection.

2. Requirement is relevant and covered by the PROFINET security concept: e.g. integrity protection of communication, confidentiality protection of communication.

3. Requirement is relevant, but depends on the field device: E.g. integrity protection of the software during SW update, integrity of the boot process (secure boot), etc.

In addition, further device-specific requirements may have to be added, which are to be determined during the threat and risk analysis (see section 3.1.2).

For field device manufacturers, it is important to classify the requirements of IEC 62443-4-2 accordingly so that it is clear which requirements affect the manufacturer itself. The PROFINET security concept provides an essential building block for securing PROFINET communication. However, it should be noted that the device manufacturer must also consider other security requirements that affect the device itself. The CB/PG10 PROFINET Security working group of PROFIBUS & PROFINET International is currently developing a table that will provide an appropriate classification. This table will be made available to the general public in due course.

It should also be noted that the IEC 62443-4-2 standard defines additional requirements (requirement enhancements) for increasing security levels. The target security level must therefore be considered when analyzing the requirements in detail.

4. Summary

This article provides an introduction and a rough overview of the two standards IEC 62443-4-1 and IEC 62443-4-2. In any case, it is necessary to refer to the standards for further work.

Using the example of an Ethernet-APL transmitter, the preceding chapters have shown that field device manufacturers have to master two essential tasks. On the one hand, the development processes must be aligned with the secure development life cycle according to IEC 62443-4-1 [12]. On the other hand, the component requirements according to IEC 62443-4-2 [13] must be observed in the development of hardware and software. PROFIBUS & PROFINET International provides the essential building blocks for secure operation of the PROFINET communication within the context of the current PROFINET specification. Nevertheless, when developing their components, manufacturers of Ethernet-APL transmitters must observe a number of other requirements that are not covered by the PROFINET protocol.

Once the two parts of the standard have been implemented, manufacturers can get the development organization and the product certified. This certification is carried out by a certifying body. It should be noted that recurring audits are required in addition to the initial audit.

5. Acknowledgement

The results of this article are based on the work of the CB/PG10 PROFINET Security working group. The authors would like to thank the working group members for their contribution, without which this article would not have been possible.

6. References

[1] PROFIBUS Nutzerorganisation e.V.: Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO. Version 2.4 MU4 Order No. 2.722, 2023. https://www.profibus.com/download/profinet-specification.

[2] PROFIBUS Nutzerorganisation e. V.: Application Layer services for decentralized periphery. Technical Specification for PROFINET IO, Version 2.4 MU4 - Nov. 2022 No. 2.712, 2023. https://de.profibus.com/downloads/profinet-specification/.

[3] PROFIBUS Nutzerorganisation e.V.: Security Extensions for PROFINET. PI White Paper for PROFINET, Karlsruhe 2019. https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/.

[4] Niemann, K.-H.: IT security extensions for PROFINET. 17th International Conference on Industrial Informatics (INDIN). IEEE 2019. PP. 407-412. DOI: 10.1109/INDIN41052.2019.897220.

[5] Niemann, K.-H., Walz, A. u. Sikora, A.: Security Extensions for PROFINET. Concepts, Status, and Prospects. Embedded World Conference 2023 Proceedings. WEKA Fachmedien GmbH 2023, pp. 99-104.

[6] Niemann, K.-H.; Walz, A.; Merklin, S.; Ziegler, D.; Waldeck, B.: PROFINET — Sichere Kommunikation im Produktionsbereich. Wie kann PROFINET zur Erfüllung der Anforderungen der IEC 62443 beitragen? In (VDI-Wissensforum GmbH Hrsg.): 24. Leitkongress der Mess- und Automatisierungstechnik Automation 2023. Transformation by Automation. VDI-Verlag GmbH, 2023; P. 391–402.

[7] Niemann, K.-H. u. Merklin, S.: OT Security Requirements for Ethernet-APL field devices. atp magazin 63 (2022) 5, pp. 44-51. DOI: https://doi.org/10.25968/opus-2288.

[8] PROFIBUS Nutzerorganisation e.V.: OT security for production plants with PROFINET - A classification of IEC 62443 for operators, integrators and manufacturers. Order No. 7.342, 2022. https://de.profibus.com/downloads/white-paper-ot-security-classification-of-iec62443.

[9] Niemann, K.-H. u. Merklin, S.: IT-Security für Automatisierungssysteme mit Ethernet-APL-Feldgeräten - Anforderungen und Schutzmaßnahmen. Automation 2022 - Automation creates sustainability. 23. Leitkongress der Mess- und Automatisierungstechnik. Düsseldorf: VDI Verlag GmbH 2022, P. 149–160.

[10] Niemann, K.-H. u. Merklin, S.: OT security requirements for Ethernet-APL field devices : Technological change can yield improved protection. atp Magazin 63 (2022) 5. https://doi.org/10.25968/opus-2288.

[11] Kobes, P.: Guide Industrial Security. IEC 62443 is easy. Berlin: VDE Verlag 2021.

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

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

[14] Department of Homeland Security: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Recommended Practice, 2016. https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[15] [15] Kuipers, D. u. Fabro, M.: Control Systems Cyber Security:Defense in Depth Strategies INL/EXT-06-11478, 2006. https://www.osti.gov/biblio/911553 .

[16] Abdelghani, T.: Implementation of Defense in Depth Strategy to Secure Industrial Control System in Critical Infrastructures. American Journal of Artificial Intelligence 3 (2019) 2, p. 17. https://doi.org/10.11648/j.ajai.20190302.11.

[17] PROFIBUS Nutzerorganisation e.V.: PROFINET Netload Robustness Guideline (former Security Level 1 Netload). No. 7.302, 2022. https://www.profibus.com/download/profinet-netload-robustness-for-security-guideline-former-security-level-1-netload.

[18] Broekman, B. u. Notenboom, E.: Testing embedded software. London: Addison-Wesley 2008.

[19] Grünfelder, S.: Software-Test für Embedded Systems. Ein Praxishandbuch für Entwickler, Tester und technische Projektleiter. dpunkt.verlag 2013.

[20] Vigenschow, U.: Testen von Software und Embedded Systems - Professionelles Vorgehen mit modellbasierten und objektorientierten Ansätzen. Heidelberg: dpunkt.Verlag 2010.

[21] ISO/IEC FDIS 30111:2019(E):2019-07. Information technology - Security techniques - Vulnerability handling processes.

[22] ISO/IEC 29147:2018(E):2018-10. Information technology - Security techniques - Vulnerability disclosure

[23] Fuhr, David et al.: Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau. 2016. https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/vdma-security-automation.html

AUTHORS

Prof. Dr.-Ing. Karl-Heinz Niemann (born 1959) represents the areas of process informatics and automation technology at Hannover University of Applied Sciences and Arts (HsH) since 2005. Since the beginning of 2023, he is member of the board of the Institute for Sensor and Automation Technology at HsH. In addition, he is active in the Mittelstand Digital Center Hannover and in the Future Lab Production of the ZDIN. From 2002 to 2005, he was responsible for the area of process data processing at the University of Applied Sciences Northeast Lower Saxony (now Leuphana University). Before that, he held leading positions in the development of process control systems at ABB, Elsag Bailey and Hartmann & Braun.

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

Dipl.-Phys. Andreas Walz is a research associate at the Institute for Reliable Embedded Systems and Communication Electronics (ivESK) at Offenburg University of Applied Sciences. His research areas include cybersecurity in industrial automation systems. In addition to his participation in the work within the PI working group CB/PG10 Security, he is an active participant in other industry working groups, such as IG securety/security at CAN in Automation e. V. and the Industrial Ethernet Security Harmonization Group, a group of cybersecurity experts from OPCF, FieldComm Group, ODVA, and PI.

Sc. Simon Merklin (born 1989) is Product Owner Security and Leader of Product Security Marketing at Endress+Hauser. He studied Information Systems at the Karlsruhe Institute of Technology with a focus on security and cryptography and wrote his master‘s thesis on Distributed Ledger Technologies. He was also involved in Endress+Hauser‘s IEC 62443-4-1 certification and is a member of the PROFINET Security Working Group at PROFIBUS and PROFINET International.

Dr.-techn. Dominik Ziegler is a Security Expert at Siemens AG. His focus is on industrial communication security. He heads the PI working group CB/PG10 Security, which deals with the development of security standards and protocols for industrial automation systems based on PROFINET.
In addition to his work on communication standards development, he is also concerned with the impact of national regulations such as the EU CRA and international standards such as IEC 62443.

Dipl.-Ing. Boris Waldeck, is Master Specialist Security PLCnext Technology and Product Solution Security Expert at Phoenix Contact Electronics GmbH in Bad Pyrmont. He is responsible for the IEC 62443-4-1 SDL certification of the Automation Systems BU and the IEC 62443-4-2 product certification of the PLCnext Control. As a PSSE, he supports the introduction of the SDL and product certifications according to IEC 62443 with a view to the upcoming EU legal regulations CRA and NIS2.