Security Extensions for PROFINET

PI White Paper for PROFINET

Version 1.05 – Date: Feb. 12, 2019

File name: PROFINET_Protocol_Security_Whitepaper_engl_V105_Feb19

Comments to be submitted to WG editor: Karl-Heinz.Niemann@Hs-Hannover.de

Prepared by PI Working Group Security “CB / PG 10”

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 trademarks. The use is restricted to members of PROFIBUS & PROFINET International. More detailed terms for the use can be found on the web page https://www.profibus.com/download/. 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-Strasse 7
76131 Karlsruhe
Germany
Phone : +49 721 / 96 58 590
Fax: +49 721 / 96 58 589
E-mail: info@profibus.com
Web site: www.profibus.com

Contents

1 Motivation 6
2 Purpose of this document 7
3 Current status PROFINET Security 8
4 Procedure 8
5 Security requirements for PROFINET 8
5.1 Security objectives/security measures 9
5.2 Delineation of the requirements and of the actors 10
5.3 Remaining requirements on the PROFINET protocol extension 11
6 Description of the concept for a PROFINET protocol security 17
6.1 Object under consideration 17
6.2 Definition of security classes 18
6.3 Migration strategy 19
6.4 Fundamental description of the main concepts 20
6.4.1 Use of certificates 21
6.4.2 System power-up 22
6.4.3 Safeguarding the cyclic messages 23
6.5 Description of the measures for PROFINET 23
6.5.1 Module basics 24
6.5.2 RTA/RTC module 25
6.5.3 AR/RPC module 25
6.5.4 Trust module 25
6.5.5 Supervisor module 25
6.5.6 GSD module 25
6.5.7 Test module 26
6.5.8 Manufacturer/vendor module 26
7 Summary and outlook 27
8 List of references 28

List of figures

Figure 1: Horizontal and vertical integration in a sample company 6
Figure 2: Transformation of the system structures 6
Figure 3: Connection of several cells to a superimposed level 7
Figure 4: Actors in the IT security process and the associated parts of IEC 62443 10
Figure 5: Delineation of product supplier and PI, primary tasks 11
Figure 6: PROFINET example system 17
Figure 7: Communication relations in the example system 18
Figure 8: Components with certificates 21
Figure 9: Authenticity verification of the public keys via certificates 21
Figure 10: Authenticity check of the devices by means of manufacturer certificate 22
Figure 11: System power-up in two phases 22

List of tables

Table 1: Security objectives of IT security 9
Table 2: PROFINET-specific security-objectives 12
Table 3: PROFINET security classes for IT security 19
Table 4: Module categories for PROFINET security 24

Change history

Version	Author	Date	Change notice
1.0	Karl-Heinz Niemann	15.12.2018	First version after WG Release for PI internal review
1.01 to 1.03	Karl-Heinz Niemann		Version Numbers skipped
1.04	Karl-Heinz Niemann	12.02.2019	Changes due to document review transferred from German version 1.04 to English version 1.04
1.05	Karl-Heinz Niemann	12.02.2019	Version cleanup. Change Tracking remove. Release candidate for advisory board review

Abstract

Within the scope of the far-reaching digitization of production processes, the IT security of production plants is gaining in importance. The pervasive networking in companies, the vertical integration and the trend toward flatter system hierarchies require comprehensive approaches for IT security in production. Previous concepts, which relied primarily on isolating the production plants, must be supplemented with new concepts that make provision for the protection of components.

PROFIBUS & PROFINET International (PI) recognized this necessity and tasked the CB/WG 10 Security working group with the development of a concept. This document provides an initial look at the results of the work thus far. It is intended to serve as a starting point for a discussion with manufacturers, integrators and users. The objective of this discussion is a coordinated and viable concept that will make industrial communication with PROFINET fit for the requirements of the future.

This document first describes the motivation and the procedure for the development of a security concept. Next, the security requirements are determined and the actors in the security process named and distinguished from one another. This document then discusses the necessary additions to the PROFINET protocol and the additional protocols required for the system startup. The points at which changes will be necessary are described at the end. The document closes with a list of the specifications that are going to be changed and an outlook for the further course of action.

1 Motivation

Industrial communication with Industrial Ethernet protocols such as PROFINET, including in the context of Industry 4.0, is growing in importance. Horizontal and vertical networking in companies will further increase in the future.

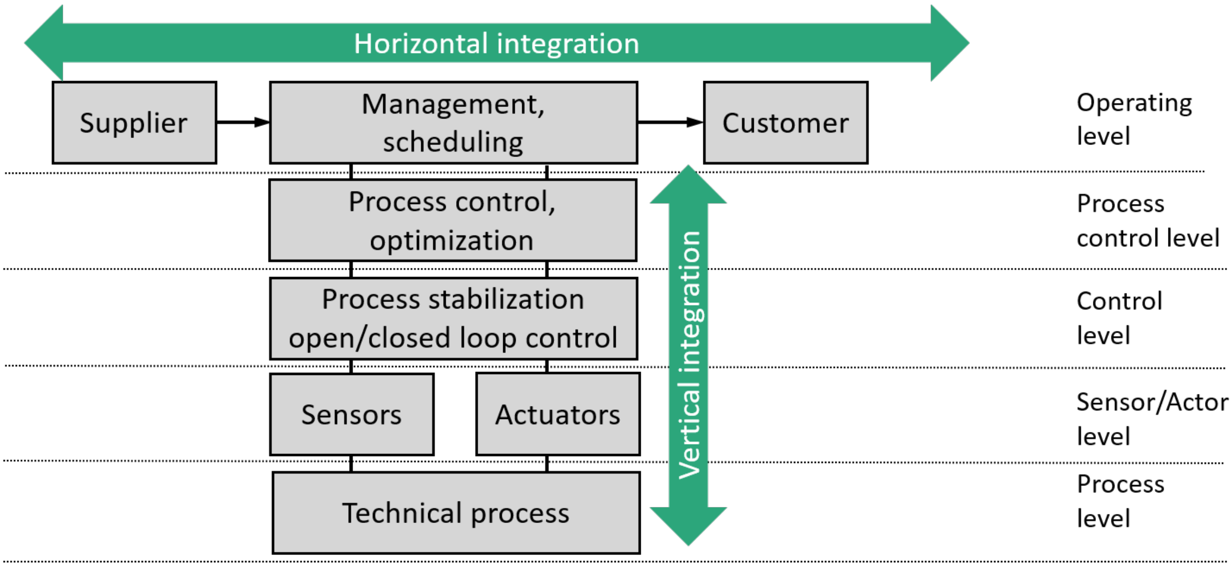

Figure 1: Horizontal and vertical integration in a sample company

Figure 1 uses a classic automation structure as an example to show the horizontal and vertical integration in a sample company. In the horizontal integration, the manufacturing company is connected to both its suppliers as well as to customers beyond its company walls through data. Production data is exchanged across company borders. With vertical integration, information is communicated not only to the next higher level, but also across layer borders.

The number of communication-capable components will increase. Ensuring the IT security of production plants will be viewed as the key requirement for future automation solutions [VDE2016]. This requirement must also be met by real-time industrial systems, such as PROFINET. IT security is a fundamental part of the Industry 4.0 strategy of PROFIBUS & PROFINET International (PI). For this reason, the CB/WG 10 Security PI working group is currently focused primarily on this topic.

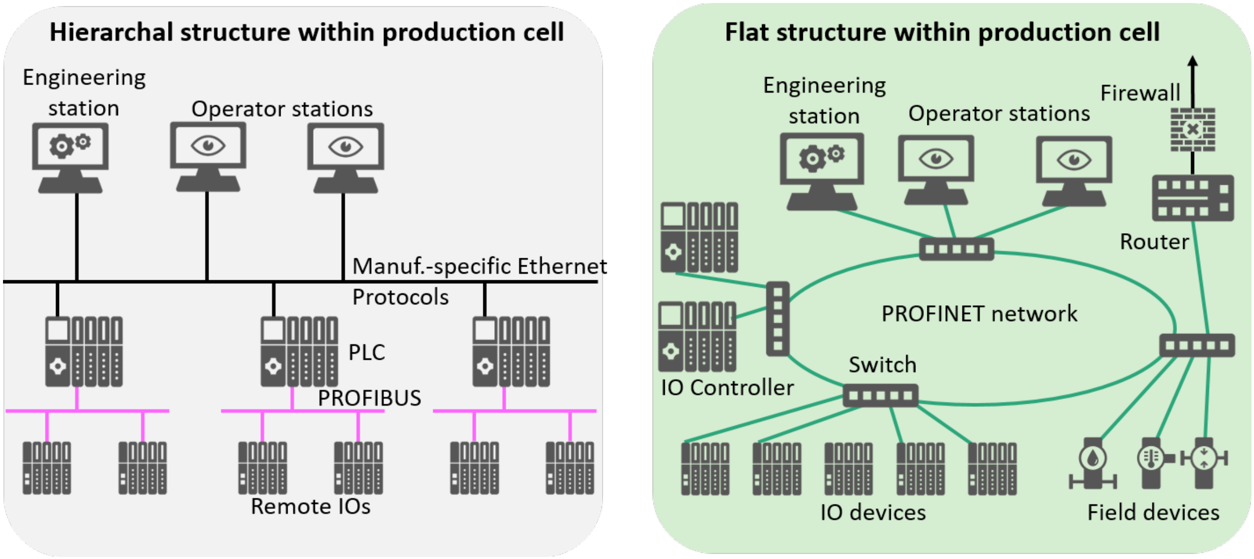

Figure 2: Transformation of the system structures

Figure 2 shows the transformation of the system structures and the elimination of hierarchies in the automation network. Shown on the left side is a hierarchal structure, such as is found in, e.g., PROFIBUS-based automation systems. Engineering and operator stations, as well as programmable logic controllers (PLCs), communicate via the automation network frequently via a manufacturer-specific protocol. The programmable logic controllers communicate with the remote IOs via PROFIBUS.

This means that different protocols are used at different levels of the network. The right side of the picture shows a structure with a uniform protocol within a production cell, as used for Industrial Ethernet systems such as PROFINET. All components are connected to a network and use the PROFINET protocol, for example. Frequently, several such cells are connected to a higher-level system (vertical integration) as shown in Figure 3.

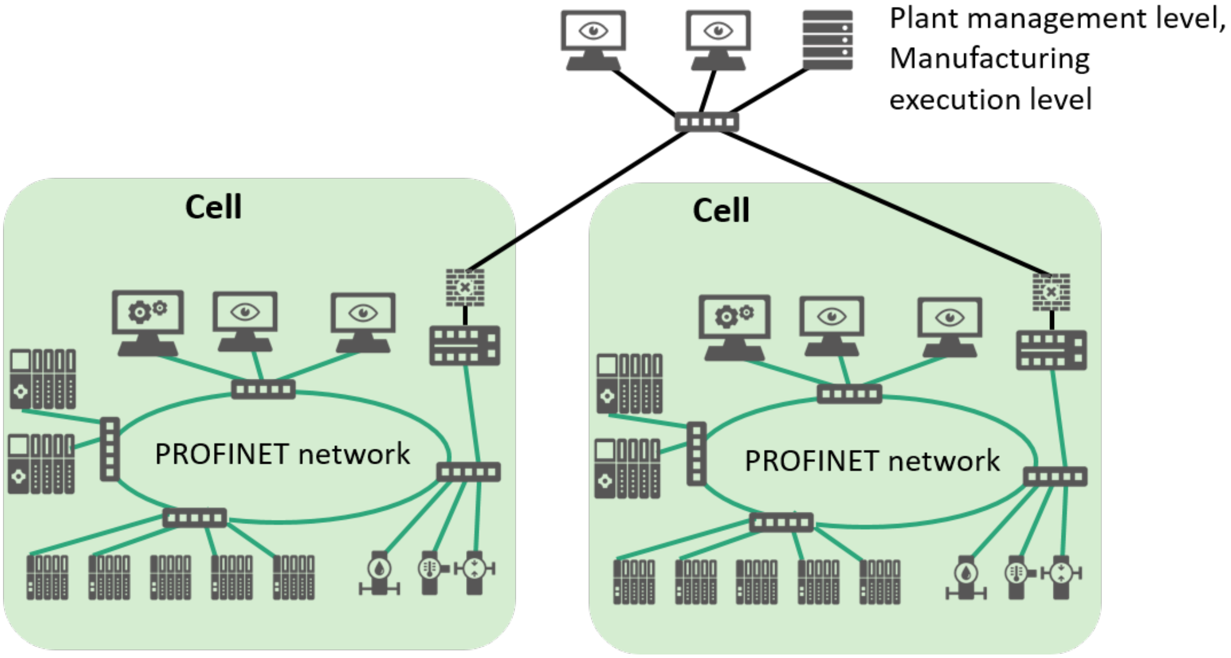

Figure 3: Connection of several cells to a superimposed level

In the future, intelligent field devices (e.g. temperature transmitters, pressure transmitters) will also communicate directly via PROFINET and with higher-level systems.

The system structure with one unified protocol offers direct accessibility to all components in the system. Network management is simplified. A connection to higher-level systems, but also direct access to the components, is easily possible. This homogeneous structure does, however, pose challenges with respect to the IT security. All components, including IO devices – a.k.a. remote IOs and intelligent field devices – can be accessed by potential attackers directly via the network. In the future, this will result in additional requirements on these devices in the event that attackers penetrate the automation network or in the case of an internal attack on the network.

2 Purpose of this document

This document is intended to provide component manufacturers, system manufacturers and users with an initial look at the planned protocol extensions and to document the underlying considerations and concepts. In addition to safeguarding the communication, special focus is put on maintaining the real-time properties of PROFINET, on the ease of use, on the coexistence with existing installations and on the serviceability.

In a second step after publication and discussion with the manufacturers and users, the corresponding specification documents are going to be created or existing specifications will be expanded. This may lead to further changes with respect to this document. This document is therefore not normative in nature. Only the subsequently released specification documents are to be considered decisive for an implementation.

3 Current status PROFINET Security

The IT security concept used for PROFINET, up to now, employs a defense-in-depth approach [DHS2016]. The production plant is protected against attacks – particularly from the outside – by means of a multi-layer perimeter that includes, among other things, firewalls [PNO2013]. In addition, further safeguarding within the plant is possible by dividing the communication network into zones. Furthermore, a security component test ensures the ability of the PROFINET components to withstand overloading in a defined scope [PNO2015]. This concept is supported by organizational measures in the production plant within the framework of a Security Management System [ISO_27001]

The described security measures correspond to what is currently state of the art. Nevertheless, further-reaching security measures will be necessary in the future. It must be noted here that internal offenders are also an increasing risk to production plants [BSI2013]. The described security measures – which focus on isolation – are effective only to a limited degree against this group of attackers. In addition, the user groups, e.g., from the process industry, demand further-reaching protection [NE_153]. PROFIBUS and PROFINET International (PI) therefore decided to protect the PROFINET protocol in the future through longer-reaching security measures on the protocol level.

4 Procedure

This document describes the work results of the PI working group CB/WG 10 Security. In previous work steps, a threat analysis was performed for PROFINET networks and the connected components within the scope of a STRIDE analysis [SHO2014]. Security objectives were derived from this and possible security measures considered. On this basis, technical solution scenarios were then analyzed and verified using defined attack scenarios. A test from the perspective of the user and a review for compliance with the fundamental requirements of IEC 62443 shall be performed after the publication of this document. Based on this procedure, the developed concept will now be presented in this document.

First a notice regarding the use of terminology: Various terms are used in documents than deal with IT security or information security. Standard [ISO_27001] speaks of information security whereas the German version of [DIN_IEC_62443-3-3] speaks of IT security. Other documents also use terms such as OT security or cybersecurity. As this document primarily references the IEC 62443 series of standards, the term IT security is used.

5 Security requirements for PROFINET

Chapter 1 described that, beyond the existing security measures, a further-reaching protection of PROFINET on the protocol level is to be developed. Moreover, it is known from [DIN_IEC_62443-3-3] that security requirements can be described in protection levels which can be achieved through the combination of technical and organizational measures. As this document focuses on protocol extensions for achieving security objectives, it is necessary to delineate between technical and organizational measures. For this reason, this chapter initially considers the security objectives from a general point of view. This is followed by a delineation to identify the necessary technical measures for the protocol extension. The chapter then summarizes the further, non-functional requirements that cannot be derived directly from security objectives.

5.1 Security objectives/security measures

Standard [DIN_IEC_62443-3-3] and other sources define the security objectives mentioned in Table 1.

Table 1: Security objectives of IT security

Security objective	Description	Relevance for PROFINET
Integrity	Property of a system for the protection against unauthorized data manipulation.	High: Message packets must not be falsified as this could, for example, lead to the unintentional activation of actuators or the recording of incorrect measured values.
Confidentiality	Information is only accessible to certain users and remains hidden from third parties.	Low: The security objective “confidentiality of IO data” is estimated as low as long as no conclusions can be drawn with regard to company secrets (e.g., recipes).
Availability	Property of system, to always perform the required function.	High: Depending on the production process, there are generally high to very high availability requirements. This is especially true for critical infrastructures.
Authenticity	Unique identification of a system component and its data.	High: The authenticity ensures that the data can be uniquely assigned to its source. The components must “identify” themselves for this purpose and have a counterfeit-proof digital identify.
Authorization	Enforce the permissions assigned to an authenticated user (human user, software process or device) that allow him to perform the required actions in the automation system and monitor the use of those permissions.	High: The usage control ensures that only authorized users can intervene in the automation system.
Non-repudiation	Ability to prove the occurrence of an alleged event or activity and the person or entity causing it.	Medium: Refers to installations where traceability of user intervention is required. For example, pharmaceutical plants operated in accordance with FDA 21 CFR Part 11 [FDA2018] [TEB2015].

With the exception of the confidentiality and non-repudiation security objectives, it can be seen that nearly all security objectives for PROFINET are assessed with the relevance of “high.” To achieve these security objectives, security measures are necessary that are to be realized at various locations and by various stakeholders. The objective of this paper is to identify those security measures that can be achieved through changes or additions to the PROFINET protocol and possibly to the communication-relevant hardware as well. Other security measures, e.g., organizational security measures, are not considered as they do not reside in the area of responsibility of the manufacturers or of PI and cannot be influenced by them or by PI. The following chapter therefore deals with an assignment of the requirements to the actors to determine the security measures that are relevant for this paper.

5.2 Delineation of the requirements and of the actors

Figure 4 shows the actors in the IT security process described in the IEC 62443 series of standards and the associated parts of the standard.

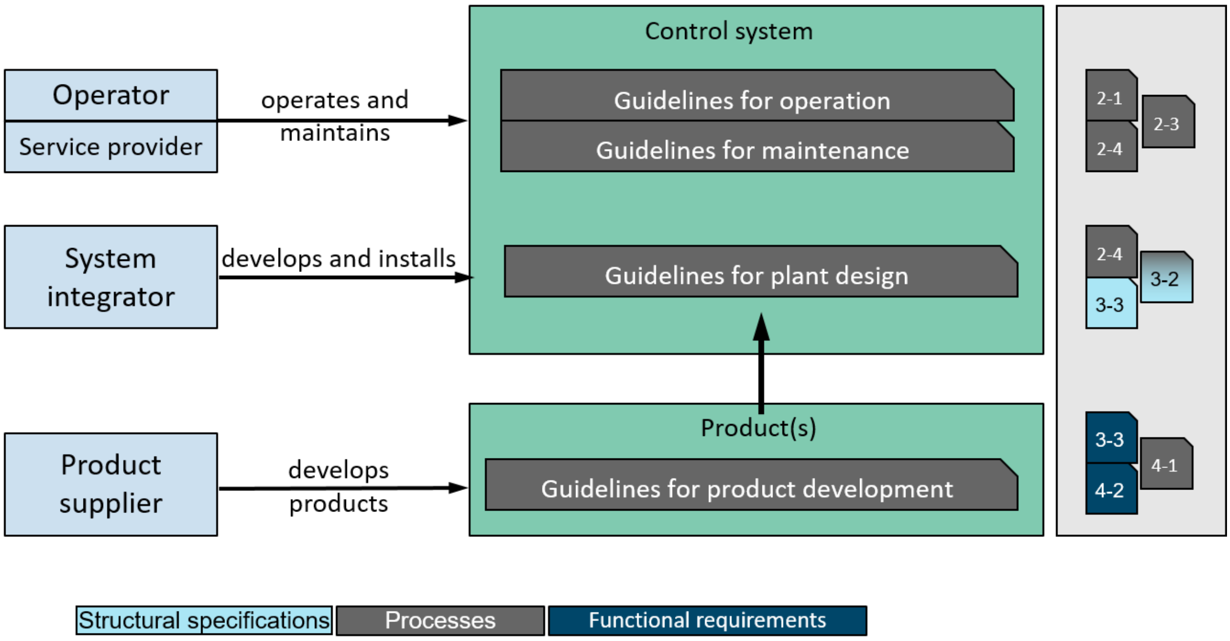

Figure 4: Actors in the IT security process and the associated parts of IEC 62443

The actors are: Operator, service provider (for maintenance), system integrator and product supplier. Figure 4 shows these with the corresponding primary activities in the security process. It can be seen that, to ensure the IT security of a production plant, the coordinated interaction of all three actors is necessary to achieve a high security level.

The operator of the system is, according to [IEC_62443-2-1], responsible for the organization of the IT security processes. This includes, e.g., the training of the personnel, the establishment of guidelines, the management of access rights, the assurance of the physical and environment-related security as well as the patch management according to [IEC_62443-2-3]. A full list of the tasks can be found in the cited standards.

This document considers the requirements that the production suppliers are to fulfil. For this reason, organizational and planning-related aspects are not considered further here. For these points, please refer to [PNO2013].

In a subsequent step, the requirements for the product suppliers are now further broken down into general requirements that are to be realized by the manufacturer and into PROFINET protocol-related requirements that apply independent of manufacturer and are defined by PI.

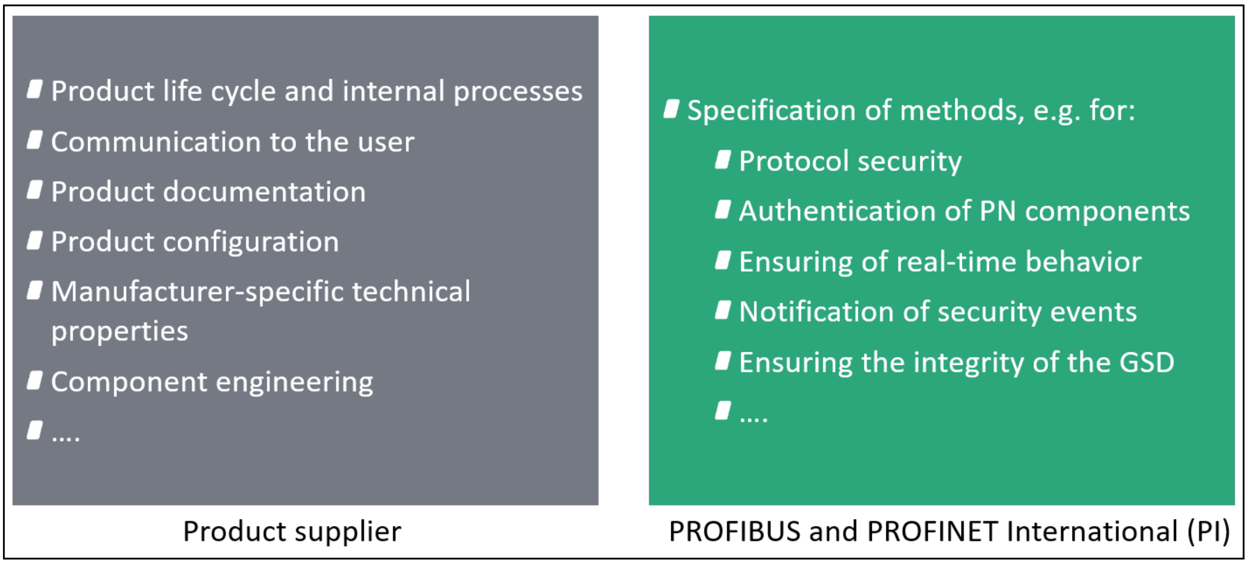
Product life cycle and internal processes
Communication to the user
Product documentation
Product configuration
Manufacturer-specific technical properties
Component engineering
....
Specification of methods, e.g. for:
Protocol security
Authentication of PN components
Ensuring of real-time behavior
Notification of security events
Ensuring the integrity of the GSD
....
Product supplier
PROFIBUS and PROFINET International (PI)

Figure 5: Delineation of product supplier and PI, primary tasks

Figure 5 shows a delineation of the responsibilities [DIN_EN_62443-4-2] between the individual manufacturers and PI. It can be seen that the generic requirements with respect to the development process, the communication with the user, the product documentation, the production configuration, etc., are in the scope of responsibility of the manufacturer. In this regard, this document provides only recommendations for the manufacturers. The responsibility of PI includes the non-proprietary functionality of PROFINET with regard to protocol extensions for ensuring the security objectives defined in Table 1. The document will focus on this in the following.

5.3 Remaining requirements on the PROFINET protocol extension

As the delineation in the previous chapter 5.2 shows, only those aspects that can be considered from a non-proprietary perspective and with respect to the PROFINET protocol are to be considered in the following. Table 2 maps the generic security objectives defined in Table 1 to PROFINET-specific security objectives. The requirements are sorted according to the operating phases of a PROFINET system (configuration, startup, operation) and according to the generic security objectives (integrity, availability, confidentiality, authorization, non-repudiation).

Table 2: PROFINET-specific security-objectives

No.	Operating phase	Generic security objective	Specific security objective	Priority	Comment
1	Operation	Integrity	The user-specified operation (established application relation, consisting of IO data, alarms and record data) of an IO controller with a configured IO device must not be falsified or changed.	high	Prevention or detection of data manipulation, suppression of alarms. Protection against unauthorized access to the components.
2	Operation	Integrity/ Authenticity / Authorization	Unauthorized access of an IO supervisor or tampering with the data transferred by the IO supervisor is to be prevented.	high	During running operation, an IO supervisor can change the configuration of the IO device, read and write acyclic data, read inputs as well as set outputs.
3	Operation	Integrity	The integrity of the clock synchronization is to be ensured	medium	Falsification of the time could lead to faulty information during signal sequence acquisition (sequence of events).
4	Operation	Integrity	The integrity of the PROFINET IRT clock synchronization (or TSN synchronization in the future) is to be ensured	high	If the integrity is violated, the real-time behavior of the system is not ensured.
5	Operation	Availability	The availability of an existing communication relation between IO controller and IO device (established application relation consisting of IO data, alarms and record data) is to be ensured.	high	Resistance against interference (e.g., overload/denial of service or manipulated data packets) has to be ensured within certain limits. E.g., by prioritizing the real-time communication during processing or by deactivating unnecessary services. Note: Part of these measures lies with the implementer.
6	Operation	Availability	The availability of redundancy functions, e.g., media redundancy, is to be ensured	medium	The security concept must also include redundant communication networks.

No.	Operating phase	Generic security objective	Specific security objective	Priority	Comment
7	Operation	Confidentiality	Confidentiality of the cyclic and acyclic IO data has to be ensured	low (for most applications)	Only relevant if information about company secrets (e.g., production recipes, 3D printer data, etc.) can be obtained from the IO data.
8	Operation	Confidentiality	The confidentiality of the device and module identification (serial number, order number, manufacturer)	low	Information can be used to prepare for an attack. A balance must be found between the need for network diagnostics and protection against spying.
9	Operation	Confidentiality	It must not be possible to read out the network topology	low	Balance between the need for network diagnostics and protection against spying on the network.
10	Operation	Confidentiality	The confidentiality of the clock information (SoE, IRT, TSN) is to be ensured	No requirement	----
11	Operation	Availability Confidentiality Integrity	The availability, confidentiality and integrity of diagnostic data provided by PROFINET components via the Simple Network Management Protocol (SNMP) has to be ensured.	low	The interface is used for the connection of network management systems and is not relevant for real-time operation. The priority is therefore low.
12	Startup	Integrity / Authenticity	The identity of a PROFINET device (station name, IP address, subnet mask) is to be ensured. (DCP features)	low	In the future, secure identification of the device will take place through a cryptographically secured process. Cryptographic safeguarding of the previously used DCP process is therefore not considered as necessary.
13	Startup	Integrity	The integrity of the configuration data that are transferred from an IO controller to an IO device is to be ensured.	high	Falsification of the configuration data could be used to transfer invalid data from an IO device to the IO controller undetected.

No.	Operating phase	Generic security objective	Specific security objective	Priority	Comment
15	Startup	Integrity	The integrity of the IP network configuration (DCP) is to be ensured prior to establishing a communication relation.	low	An attack during network configuration can result in traffic being redirected. Priority is set to low, as through end-to-end security, attacks will be detected at a later point in time.
16	Startup	Integrity	The integrity of the PROFINET network configuration (NoS) is to be ensured prior to establishing a communication relation.	low	An attack during network configuration can result in traffic being redirected. Priority is set to low, as through end-to-end security, attacks will be detected at a later point in time.
17	Startup	Availability	The availability of an established communication relation must be ensured following a power failure.	high	Automatic restart following a power failure.
18	Startup	Confidentiality	The confidentiality of the configuration data that are transferred from an IO controller to an IO device has to be ensured.	medium	An attacker can use the configuration data to obtain information about the structure of the IO data and use this for an attack.
19	Startup	Confidentiality	The confidentiality of the IP network configuration has to be ensured prior to establishing a communication relation.	not a security objective	There is no critical information in this item that needs confidentiality.
20	No assignsignment	Confidentiality	The confidentiality of the PROFINET network configuration (NoS) has to be ensured prior to establishing a communication relation.	not a security objective	---
21	No assignsignment	Authenticity	An IO device must not be controlled by an IO controller other than intended in the planning.	high	Prevention of a man-in-the-middle attack.

No.	Operating phase	Generic security objective	Specific security objective	Priority	Comment
23	No assign-signment	Confidentiality	The confidentiality of private keys has to be ensured when using cryptographic processes.	high	If the confidentiality is breached, network nodes could use a false identity.
24	Engineering	Integrity/ authenticity	The integrity and authenticity of the data in the device master file (GSD file) have to be ensured.	high	Falsification of the GSD could be used to transfer invalid data from an IO device to the IO controller undetected by the IO controller. This also applies in the opposite direction.
25	Engineering	Confidentiality	The confidentiality of the data in the device master file (GSD) has to be ensured.	not a security objective	---
26	Mainte nance	Integrity	The integrity of the firmware in an IO controller is to be ensured	high	Is to be solved on a manufacturer-specific basis
27	Mainte nance	Integrity	The integrity of the firmware in an IO device is to be ensured	high	Is to be solved on a manufacturer-specific basis

The PROFINET-specific security objectives in Table 2 are to be supplemented with further requirements that cannot be allocated directly onto to the generic security objectives. These include the following:

- The real-time behavior of the PROFINET system must also to be ensured when security measures are implemented. Note: As the planned cryptographic measures in the PROFINET devices demand additional computing power, it has to be assumed that the security measures could – when using the same hardware equipment – affect the cycle time.
- The security measures that are used must be state of the art.
- Where possible, the security measures should be updatable via a software update when they are not any longer state of the art.
- The security concept should take into account economic considerations. These include: Cost for the implementation, cost for maintenance, time to market.
- The coexistence of PROFINET components with and without security measures must be possible. An attacker must not be able to force unsecured operation, however.

- The replacement of defective devices during operation without the need to use an engineering tool must still be possible.

- After a power failure, a system must be able to start up without connection to the Internet (black start capability).

- During operation, there should be no need for additional permanently installed system components. Additional components for startup of system (PKI, validation of certificates) might be required.

- The existing PROFINET profiles, such as PROFIsafe, must be usable without restriction.

- The IT security solution that is to be defined should be scalable so that it can be adapted to the requirements of various users.

- The solution to be defined must take into account the installed basis. Compatibility with existing installations has to be ensured. The addition of components that are equipped with activated IT security features must not endanger the operation of an existing system.

The appropriate security measures are derived from these requirements and the corresponding prioritization in the next chapter.

6 Description of the concept for a PROFINET protocol security

The following chapter describes the basic concepts with which a PROFINET system is to be protected in the future. At this point in time, this concept initially represents a work approach that may still change in the course of further technical evaluation. In chapter 6.1, a simple PROFINET system is first defined which will serve as the basis for the considerations. Chapter 6.2 then defines security classes as not all security requirements apply for all systems. Chapter 6.3 presents a migration strategy for existing installations. Chapter 6.4 describes the fundamental concepts. This is followed in chapter 6.5 with a description of the selected security measures based on so-called building blocks. The chapter concludes with additional measures for manufacturers and operators.

6.1 Object under consideration

For the further considerations, a PROFINET system is first defined. This is shown in Figure 6. The system is operated within the framework of the cell protection concept described in chapter 3.

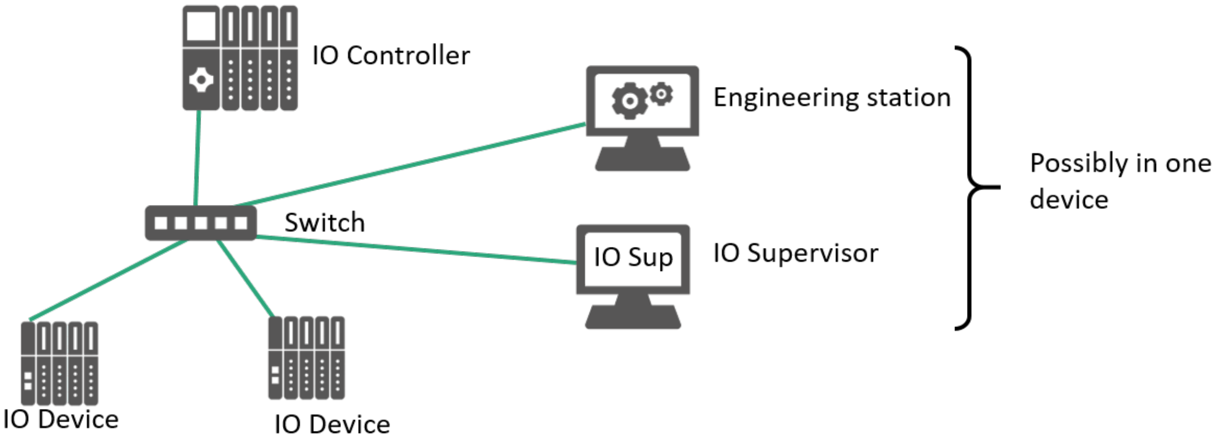

Figure 6: PROFINET example system

The example system consists of an IO controller with two allocated IO devices and a switch. The engineering station is used to configure the system. In addition, an IO supervisor is connected to the system. Human users exist for both systems, to whom corresponding user roles can be assigned if required. This may be, e.g., an additional tool for commissioning or for the diagnosis of the bus system. In many cases, the engineering tool simultaneously performs the function of the IO supervisor. Although a separate switch is possibly not necessary in many systems because the components are equipped with integrated switches, this is considered here as well. This is necessary since the switch may also contain configuration data, e.g., with respect to virtual networks. A switch without PN functionality is used in the example system. In addition to its switch functionality, this also features the properties of a PROFINET IO device. As a result, the switch can transfer certain status information via the PROFINET protocol to the IO controller, to the engineering station or to the IO supervisor.

Communication relations exist between the components of the systems shown in Figure 6. These are shown in Figure 7.

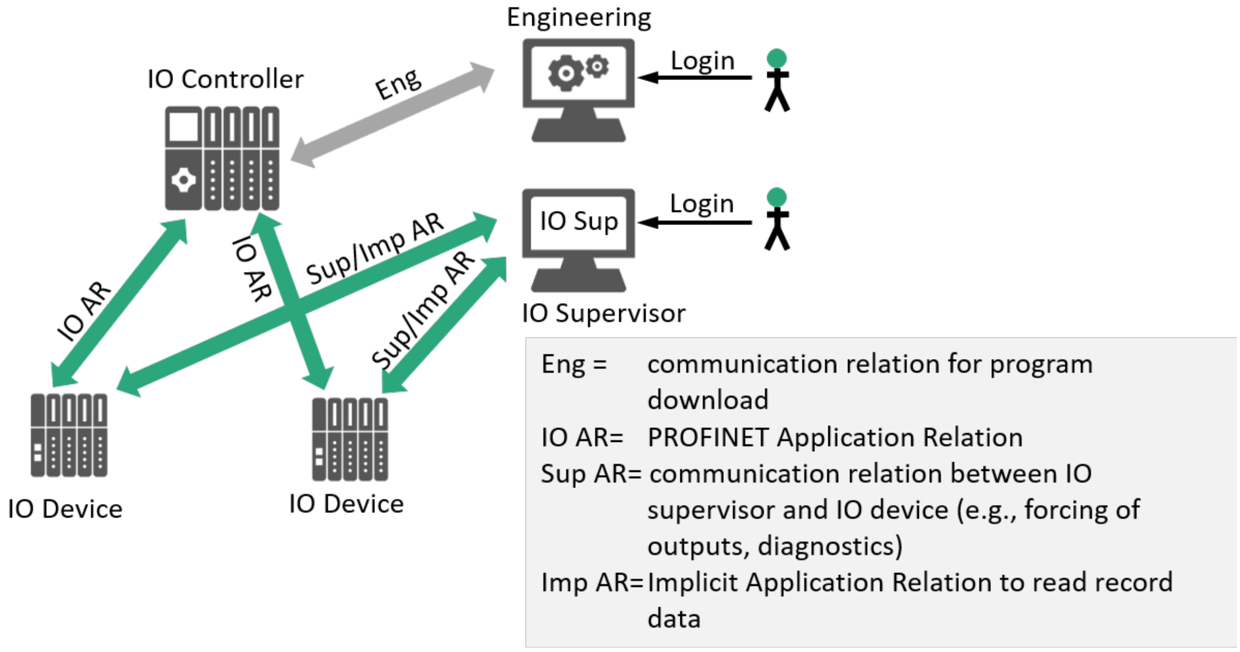
Engineering
Login
IO Controller
Eng
IO Sup
Login
Sup/Imp AR
IO AR
IO AR
Sup/Imp AR
IO Supervisor
IO Device
IO Device
Eng = communication relation for program download
IO AR= PROFINET Application Relation
Sup AR= communication relation between IO supervisor and IO device (e.g., forcing of outputs, diagnostics)
Imp AR= Implicit Application Relation to read record data

Figure 7: Communication relations in the example system

From the perspective of PROFINET, the PROFINET IO Application Relations (IO AR) are of interest. The IO controller and the IO device exchange cyclic and acyclic data as well as alarms via the IO AR. Parallel to this, an IO supervisor can establish a communication relation with the IO devices (Sup AR) to, e.g., perform diagnostics, read IO data or manually set IOs for commissioning purposes.

In addition to these PROFINET-specific communication relations, the engineering station has a communication relation to the IO controller to, e.g., load this with the control programs (shown as Eng in the figure). Access data (logins) is generally required for both the engineering station as well as for the IO supervisor in order to use the stations.

In the following description of measures for safeguarding a PROFINET system, the explained assets and the corresponding communication relations are used as a basis. The IO ARs and Sup ARs are the focus of this document. The connection between Engineering and IO Controller (Eng) is given consideration as well, but is the responsibility of the manufacturer.

6.2 Definition of security classes

The analysis of the PROFINET security objectives in Table 2 shows that the security objectives were given varying priority. This is true especially for the aspect of confidentiality. The confidentiality security objective is only relevant in certain application cases in which it is possible to obtain information about company secrets by reading the IO data. It is known from [RUN2014a] that the computing power for ensuring the confidentiality (encryption) is significantly higher than for ensuring the integrity, e.g., through cryptographic checksums. Moreover, it is to be assumed that most applications do not have confidentiality of the cyclic IO data as a security objective. For this reason, three security classes are defined according to Table 3.

Table 3: PROFINET security classes for IT security

Security class	Name of the security class	Definition	Typical area of application
1a	Robustness	Current status of PN security according to chapter 3 and in addition: SNMP default strings can be changed, DCP commands can be set to "read only," GSD files are protected against changes by signatures.	Incremental improvement in relation to current status of PN security. It must still be discussed whether this class is to be introduced.
2	Integrity + Authenticity	In addition to the requirements of security class 1, the integrity and authenticity of the assets and of the communication relations are secured by means of cryptographic functions. The confidentiality of the configuration data is ensured. The confidentiality of the IO data is not necessary.	Isolated systems with communication relations to the outside. System cannot or not easily be divided into zones separated from each other. Access to the installation cannot be secured (e.g., installation is outdoors without permanently present personnel). Application places no requirements with respect to the confidentiality of the IO data.
3	Confidentiality	In addition to the requirements of security class 2, the confidentiality of the communication relations is ensured.	Installation according to security class 2 in which information about company secrets can be obtained from the IO data of the system.

The right column in Table 3 shows the typical areas of use for the three security classes.

Security class 1 provides short-term incremental improvements in relation to the current status of PN security described in chapter 3.

Security class 2 is intended for installations that have a higher level of communication to areas outside of the installation or in which access to the system can not be monitored as well. This class is used if the operator has higher IT security requirements on the communication via PROFINET. In this mode, the cyclic services are protected against unauthorized modifications. At the same time, the trustworthiness, integrity and authenticity of the acyclic services are ensured.

Security class 3 ensures integrity, authenticity and confidentiality of all services. It is assumed that security class 3 is only used in those cases where information about company secrets can be obtained by reading cyclic IO data. Note: The acyclic communication services of security class 2 offer an alternative for the transfer of confidential data, e.g., recipes.

Most applications are able to operate on the basis of security classes 1 and 2.

6.3 Migration strategy

Existing installations (brownfield installations) are generally built according to the description in chapter 3. The IT security is ensured via the defense in depth concept. This is generally implemented by isolating the installation to the outside, segmentation of the production network, access protection and other measures.

To introduce security class 2, hardware and software are required that meet the requirements for providing the additional security functions. Thus, the assemblies generally require higher computing power. It is to be assumed that it will not be possible to retrofit existing installations through software updates in all cases. A change to security class 2 or 3 therefore generally occurs when installations are replaced or expanded. Because mixed operation of components of all security classes will be possible, old system parts with security class 1 can be operated in parallel with system parts with security class 2 or 3 in the same network.

6.4 Fundamental description of the main concepts

From the security objectives in Table 2 and taking into consideration the conducted further analyses and underlying priorities, the following security measures can be derived for a PROFINET system:

1. Ensuring the authenticity of the PROFINET nodes through a cryptographically secured digital ID, e.g., in the form of certificates. The concept should also include the possibility to securely store this ID, e.g., in a specially secured hardware component in the respective node. For further information, see [SPE2013] [RUN2014b].

2. Ensuring the integrity of the communication through cryptographic measures, e.g., cryptographic checksums. This security measure must include all communication channels of the PROFINET node, consisting of IP communication, PROFINET real-time communication and communication for network management.

3. Ensuring system startup and the assignment of components, e.g., of IO devices to IO controllers and engineering tools, through cryptographic measures. This also applies for a system startup following a connection interruption.

4. Reporting of security-relevant events that can be detected by PROFINET devices. E.g., through additional PROFINET IT security alarms.

5. Ensuring the confidentiality of all acyclic data and of the configuration data. Additional safeguarding of the confidentiality of cyclic data as **optional** function in security class 3. Note here that the computing power for confidential communication (encryption) is significantly higher than for simple integrity protection, e.g., through a cryptographic checksum. Measured values for this can be found in [RUN2014b].

6. Ensuring the minimum requirements to protect against denial of service attacks. This aspect has already been realized acc. to [PNO2015] within the scope of netload tests. During the course of further work, it must be discussed whether a minimum requirement higher than netload class I is required.

7. Protection of the integrity and authenticity of general station description files (GSD).

Further-reaching requirements, e.g., the integrity check GSDs in an engineering tool, secure firmware and secure development process are, according to the delineation performed in chapter 5.2, to be implemented in a manufacturer-specific manner.

Furthermore, the fundamental mechanisms are described that allow secure communication to be established in a PROFINET system.

6.4.1 Use of certificates

The following chapter deals with the use of certificates as part of the PN security concept.

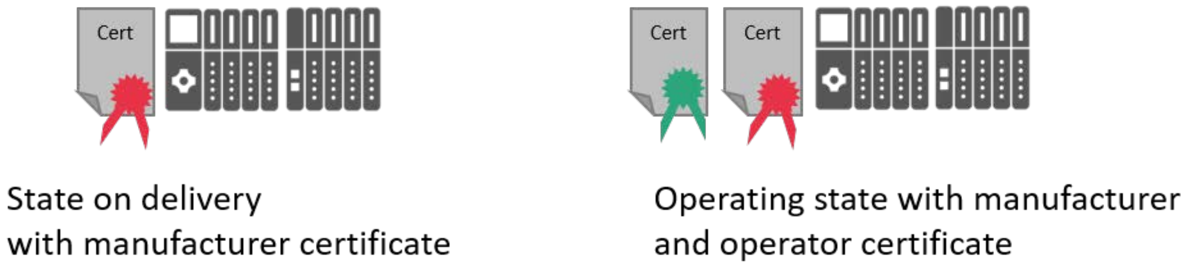
Cert
State on delivery
with manufacturer certificate
Cert
Cert
Operating state with manufacturer
and operator certificate

Figure 8: Components with certificates

Figure 8 on the left shows the delivery status of an IO component (IO Device, IO Controller) as supplied by the manufacturer. A manufacturer certificate, shown in red in the picture, should be stored in this component. This allows the operator to check the authenticity of the device. This provides protection against unauthorized copying. When the operator takes over the component, he must supplement his own operator certificate, shown in green in the figure. At the same time, the operator can integrate the device into his own public key infrastructure (PKI) via his operator certificate.

The certificate contains the public key of the component. As shown in Figure 9, the authenticity of the public keys is verified using the certificates and digital signatures. In this case, the operator certificates are shown in the figure. The keys and device certificates can be managed via a public key management function, such as is integrated in the engineering tool.

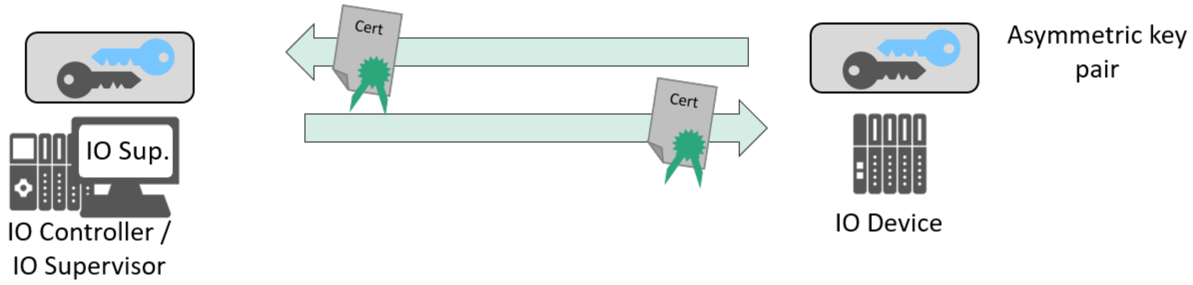

Figure 9: Authenticity verification of the public keys via certificates

Based on this authentication, the symmetric keys are then created and exchanged.

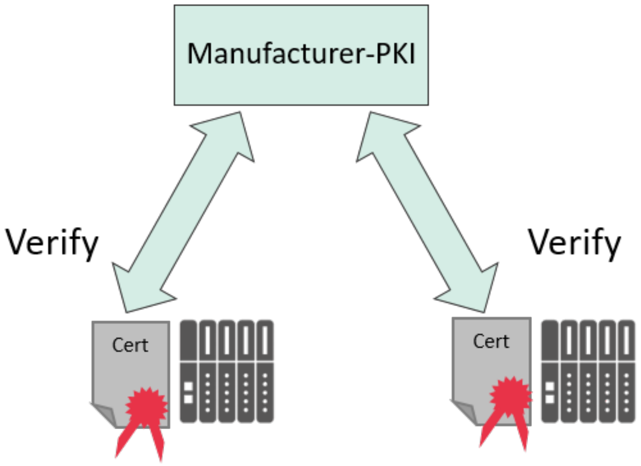

Figure 10: Authenticity check of the devices by means of manufacturer certificate

As can be seen in Figure 10, the authenticity of the manufacturer certificates can be checked in regular intervals. This check allows certificates to be revoked by the manufacturer if necessary. Currently under discussion is whether PROFIBUS & PROFINET International (PI) will define the mechanisms for the authenticity check.

6.4.2 System power-up

As shown in Figure 11, a secured PROFINET system is powered up in two phases.

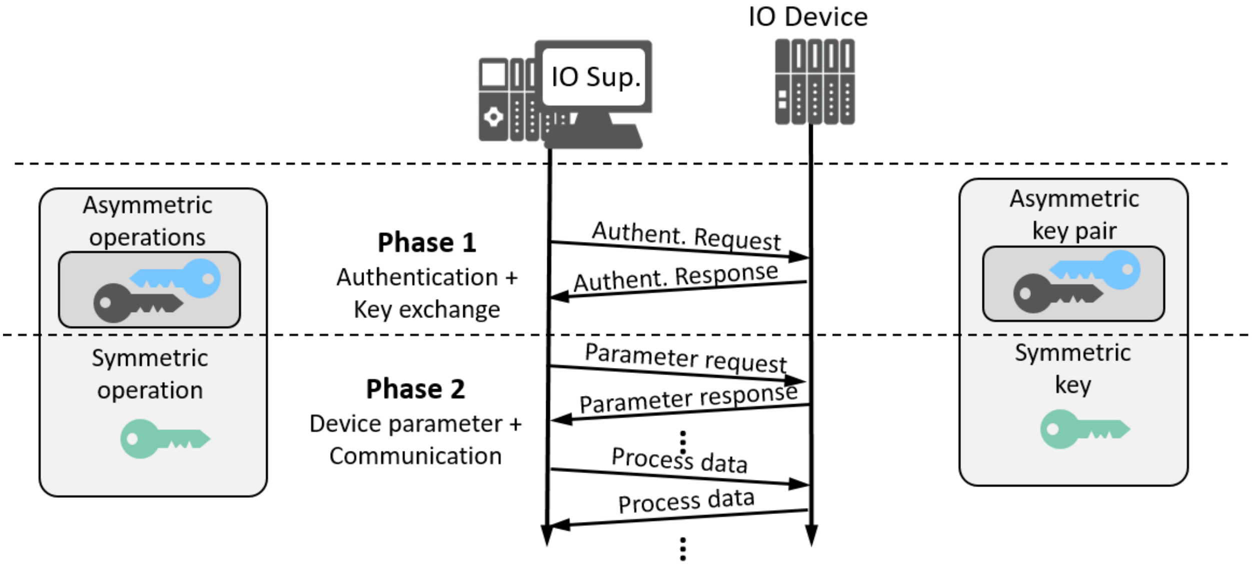

Figure 11: System power-up in two phases

In phase 1, a private/public key process is first used for mutual authentication and to exchange keys between the IO controller or the IO supervisor and the IO device. To do this, the nodes exchange their public keys (blue in the figure) and together negotiate symmetric keys (green in the figure) which are then used for the further communication (Phase 2). The changeover to a symmetric process is useful as this process demands less computing power than an asymmetric process. In the event of a restart, e.g. if communication is interrupted, the described procedure is repeated.

6.4.3 Safeguarding the cyclic messages

The PROFINET data packets are safeguarded via a message authentication code. A cryptographic checksum is calculated via the data packet here. By way of this measure, the integrity and authenticity of the message packet can be checked by the receiver. The calculation of the MACs uses the previously described symmetric keys in addition to a sequence counter. The advantage of this process is the relatively simple calculation of the MAC. In [RUN2014a], the suitability of various message authentication codes have been evaluated for data packets with a length typical for PROFINET. This examination has determined that the HMAC-SHA 256 algorithm [NIST198] is the best-performing solution. No final selection of MAC algorithm has yet been made. This will be determined following further discussion and testing. It is to be assumed that the algorithm will be negotiated while the connection is being established to allow for a transition to higher-performance algorithms in the future.

The content of the data packet remains readable. If necessary, encryption can optionally be performed to take into account the confidentiality security objective.

6.5 Description of the measures for PROFINET

The IT security concept outlined in chapter 6.4 builds on a number of modules, which are divided into the categories described in Table 4.

Table 4: Module categories for PROFINET security

Category	Description
Basics	Fundamental security measures
RTA/RTC	Safeguarding of the cyclic layer-2 PROFINET communication and the acyclic layer-2-based alarm mechanisms.
AR/RPC	Non-cyclic communication for establishing a connection from an IO controller to an IO device or from an IO supervisor to an IO device.
Trust	All functions that are necessary for identifying the communication partner and establishing a trust relationship.
Supervisor	Securing the connection to configuration or diagnostic tools that access an IO Device via a PROFINET read access or the reading and writing of IO parameters, or as e. g. a diagnostic tool does via an implicit AR when reading diagnostic data.
GSD	Protection of the device description file that is supplied with an IO device.
Test	Tests that are to be performed during the certification of the PROFINET devices are to be ensured in order to satisfy the security requirements according to the defined security classes, robustness and interoperability.
Manufacturer	Tasks of the manufacturer. These tasks are listed for the sake of completeness but are assigned to the manufacturer.
Documentation	Provision of security-relevant information for operators.

The following sections describe the content of the modules.

6.5.1 Module basics

This chapter describes the fundamental measures for securing PROFINET communications. The measures are:

1. Establishment of a possibility to deactivate unneeded PROFINET services. A user interface has to be provided for this purpose in the engineering tool, which can be used to deactivate unneeded PROFINET- or other services. Example: Deactivation of network management services (SNMP).
2. Generation of system alarms that indicate security-relevant events. Example: If, when using cryptographic checksums, data packets are detected whose cryptographic checksum is not correct even though the data packet itself is intact (correct CRC), a system alarm is to be triggered.
3. Limiting of the DCP service to read only. This can be used to prevent the unauthorized changing of the device name, changing of the IP address and the resetting to the factory settings.
4. Currently still in discussion: Use of secure network management services (SNMPv3). Use of access data for accessing SNMP data in devices. Setting up access protection to the network management data (community string).

6.5.2 RTA/RTC module

The RTA/RTC module defines the safeguarding of the cyclic communication via the message authentication codes described in chapter 6.4. Included here are:

1. Safeguarding of the cyclic layer-2 PROFINET communication and the acyclic layer-2-based alarm mechanisms via message authentication codes.
2. Protection against replay attacks by additional message counters or integrity protection of the existing message counters.
3. Regular renewal of the symmetric key during running operation as protection against reverse calculation of the key.
4. Option for security class 3: Additional encryption of the message.

6.5.3 AR/RPC module

The AR/RPC module is used for the secure setup and operation of the application relation. The following measures are provided for this purpose.

1. Setup of the application relation between IO controller and IO device or between IO supervisor and IO device via the asymmetric key process described in chapter 6.4. (Phase 1 acc. to Figure 11). Is used for:
   a. Establishing a connection including security handshake.
   b. Negotiating the symmetric key for cyclic and acyclic communation.
   c. Changing the symmetric key at runtime.
2. Operation of the connection using the symmetric key determined under point 1, also for acyclic non-real-time communication (e.g. record services).

Note: Authentication of the communication partners via operator certificates.

6.5.4 Trust module

The trust module handles the aspects of secure identities for assets and users as well as their secure storage. To be addressed here in particular are:

1. Provision of secure identities for users, e.g., by requiring name and password when accessing the engineering tool or the IO supervisor. The protection goals of authorization and non-repudiation are realized through this.
2. Provision of secure identities for IO devices, IO controller and IO supervisor, e.g., through manufacturer and/or operator certificates with the possibility for validating the device certificates with a manufacturer certificate.
3. Option: Prior to the transfer of the operator certificate, the identity of the device is checked via the manufacturer certificate.
4. Provision is to be made for a possibility to revoke certificates.
5. Provision is preferably to made for secure storage of the key information in specially secured hardware modules (e.g., Trusted Platform Module TPM [BSI2018]).

6.5.5 Supervisor module

The supervisor module handles the security of the IO supervisor. This applies to both the access of the operating personnel of the IO supervisor as well as to the access of the IO supervisor on the IO devices. The key measures are:

1. Authentication of the human user of the IO supervisor by means of user name and password or a centralized user management (single sign on) or with certificates as an option.
2. Integration of the IO supervisor in the secure establishment of a connection according to Figure 11.

6.5.6 GSD module

The general station description (GSD) file is a text file based on the GSDML description language, which contains the properties of PROFINET components. Provision is to be made for the following expansions for the GSD:

1. Expansion of the GSD content with information that describes the security capabilities of a PROFINET device.
2. Protection of the GSD content against changes, e.g., though a digital signature.

6.5.7 Test module

PROFINET devices of security class 1 are today already subjected to a security test within the scope of the certification process [PNO2015]. This test focuses primarily on the robustness of the devices, particularly in regard to an overload (denial of service). These tests are to be expanded in the future as follows:

1. Devices of security classes 2 and 3 must satisfy netload class II according to [PNO2015]. The need to extend the network load tests should be discussed.
2. The effectiveness of the additional security measures, e.g., the triggering of alarms in the event of security-relevant events, is to be tested within the scope of the certification. The test specification [PNO2017] is to be expanded accordingly.

6.5.8 Manufacturer/vendor module

According to the delineation laid out in chapters 5.2 and 5.3, this document distinguishes between requirements that are to be undertaken through additions to various PROFINET documents and additions that are the responsibility of the manufacturers. This section provides the manufacturers with information on which measures are to be taken by the manufacturer. In spite of these recommendations, the aspects remain the responsibility and under the decision-making authority of the manufacturer. In the following consideration, a distinction is made between component manufacturers and system manufacturers. It is assumed that system manufacturers produce all component types (IO controller, IO device, IO supervisor, engineering tool). It is assumed that component manufacturers produce only IO devices.

Component manufacturers

1. Establish a process for issuing and revoking manufacturer certificates.
2. Provide a secure storage location for key information for IO devices.
3. Establish processes for supporting a patch management system for software according to [IEC_62443-2-3].
4. Take into account the development and documentation requirements oriented towards [IEC_62443-4-1] and [IEC_62443-4-2].
5. Ensure the integrity of the software in IO devices, e.g., by signing the software, in combination with a secure boot if necessary.

System manufacturer

All requirements of a component manufacturer must be satisfied. System manufacturers must also satisfy the following points:

1. Establish a user management system with assignment of user rights for IO supervisor and engineering tool.
2. Provide a user interface for the configuration of security functions, e.g., for the deactivation of unneeded services, integrity test of the GSD. A concept for the procedure in the event that GSD integrity check is not passed or not possible should be defined and implemented by the system manufacturer.
3. Provide a secure storage location for key and other critical information for IO controller, IO supervisor and, if applicable, engineering tool. Transitional solutions are possible:
4. Provide a tool for generating operator certificates, e.g., in the engineering tool or elsewhere.
5. Ensure the integrity of the software in IO controller and IO supervisor, e.g., by signing the software, in combination with a secure boot if necessary.
6. Protect the connection between engineering tool and IO controller against tampering. Note: This communication is generally realized in a manufacturer-specific manner.

7 Summary and outlook

The information provided in this document is, for now, relatively general and less specific. In a subsequent publication, this document will serve as the basis for determining which parts of the PROFINET specifications require expansion. These will likely be:

- PROFINET Application Layer Protocol for Decentralized Periphery [PNO2018c]
- PROFINET Application Layer Services for Decentralized Periphery [PNO2018b]
- PROFINET Security Guideline for PROFINET [PNO2013]
- Test Specification for PROFINET [PNO2017]
- GSDML Technical Specification for PROFINET [PNO2018a]
- PROFINET Design Guideline [PNO2014]
- Additional document: Implementation Information for PROFINET Components (new document)

The corresponding working groups at PI will prepare the necessary changes and present them for discussion within PI. The necessary technical detailing will then be performed as well. Furthermore, prototyping is currently being discussed. Final results are not yet available.

In a next step, the specified security solutions will be mirrored on the basic requirements of the IEC 62443 standard of series and verified. Due to time constraints, this examination cannot be part of this paper.

8 List of references

[BSI2013] Bundesamt für Sicherheit in der Informationstechnik (BSI) [German Federal Office for Information Security]:Industrial Control System Security: Internal offenders. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_061.html, 29.07.2015.

[BSI2018] Bundesamt für Sicherheit in der Informationstechnik (BSI) [German Federal Office for Information Security]:The Trusted Platform Module (TPM) and trustworthy information technology. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/dastrustedplatformmoduletpm_node.html.

[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.

[DIN_EN_62443-4-2] German Commission for Electrical, Electronic and Information Technologies of DIN and VDE, German Institute for Standardisation DIN EN 62443-4-2:2017-10; VDE 0802-4-2:2017-10 - Draft: Industrial communication networks – Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components (IEC 65/663/CDV:2017); German version prEN 62443-4-2:2017. Beuth Verlag, 2017.

[DIN_IEC_62443-3-3] German Commission for Electrical, Electronic and Information Technologies of DIN and VDE, German Institute for Standardisation DIN IEC 62443-3-3:2015-06; VDE 0802-3-3:2015-06 - Draft: Industrial communication networks – Network and system security - Part 3-3: System security requirements and security levels (IEC 62443-3-3:2013 + Cor.:2014). Beuth Verlag, Berlin, 2015.

[FDA2018] U. S. Food & Drug Administration: CFR - Code of Federal Regulations Title 21, Part 11. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1.

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

[IEC_62443-2-3] IEC- International Electrotechnical Commission IEC TR 62443-2-3:2015: Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment, 2015.

[IEC_62443-4-1] IEC- International Electrotechnical Commission IEC/NP 62443-4-1: Industrial communication networks – Network and system security – Part 4-1: Product development requirements, 2013.

[IEC_62443-4-2] IEC- International Electrotechnical Commission IEC/NP 62443-4-2: Industrial communication networks – Network and system security – Part 4-2: Technical security requirements for IACS components.

[ISO_27001] DIN German Institute for Standardisation DIN ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 + Cor. 1:2014), 2015.

[NE_153] NAMUR –User Association of Automation Technology in Process Industries NE 153: Automation Security 2020 – Design, Implementation and Operation of Industrial Automation Systems, Leverkusen, 2015.

[NIST_197] NIST Computer Security Division (CSD): Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf.

[NIST198] NIST Computer Security Division (CSD): FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC), [PNO2013] PROFIBUS Nutzerorganisation e.V.: PROFINET Security Guideline Guideline for PROFINET https://de.profibus.com/downloads/profinet-security-guideline/.

[PNO2014] PROFIBUS Nutzerorganisation e.V.: PROFINET Design Guideline. https://de.profibus.com/index.php?eID=dumpFile&t=f&f=49686&token=53a58fd07df8cc843a50cdd9efd29db0c325f4e7.

[PNO2015] PROFIBUS Nutzerorganisation e.V.: Test specification PROFINET IO Security Level 1 / Netload. Technical Specification for PROFINET. http://www.profibus.com/nc/download/test-and-certification/downloads/profinet-io-net-load-1/display/, 15.07.2014.

[PNO2017] PROFIBUS Nutzerorganisation e.V.: Test Specification for PROFINET Related to PROFINET V2.35. Technical Specification for PROFINET. https://de.profibus.com/downloads/profinet-test-specification/.

[PNO2018a] PROFIBUS Nutzerorganisation e.V.: GSDML - Technical Specification for PROFINET. https://de.profibus.com/downloads/gsdml-specification-for-profinet/.

[PNO2018b] PROFIBUS Nutzerorganisation e.V.: Application Layer services for decentralized periphery. Technical Specification for PROFINET IO. https://de.profibus.com/downloads/profinet-specification/.

[PNO2018c] PROFIBUS Nutzerorganisation e.V.: Application Layer Protocol for Decentralized Periphery. Technical Specification for PROFINET IO. https://de.profibus.com/downloads/profinet-specification/.

[RUN2014a] Runde, Markus; Hausmann, Stefan; Tebbe, Christopher; Czybik, Björn; Niemann, Karl-Heinz; Heiss, Stefan; Jasperneite, Jürgen: SEC_PRO - Sichere Produktion mit verteilten Automatisierungssystemen. Schlussbericht für das FHprofUnt-Forschungsprojekt mit dem FKZ 1760A10 sowie 17060B10. https://serwiss.bib.hs-hannover.de/frontdoor/index/index/docId/499, 17.12.2014.

[RUN2014b] Runde, Markus: Echtzeitfähige Protokollerweiterung zum Schutz Ethernet-basierter Automatisierungskomponenten. (Real-time capable protocol extension for securing Ethernet-based automation components.) Dissertation submitted in fulfilment of the requirements for the degree of doctor of engineering (Dr.-Ing.). Dissertation, Magdeburg, 2014b.

[SHO2014] Shostack, Adam: Threat modeling. Designing for security. Wiley, Indianapolis, IN, 2014.

[SPE2013] Speth, Walter: Nur Befehle befolgt. CPS erfordern sichere Identitäten. In atp-edition 12, 2013; S. 46–52.

[TEB2015] Tebbe, Christopher, Niemann, Karl-Heinz, Runde, Markus: IT-Sicherheit in Pharmaanlagen. In Techno Pharm 1, 2015, Jahrgang 5; S. 34–39. https://www.ecv.de/download/download/Zeitschriften/TechnoPharm/volltext/TP0501_0327.pdf

[VDE2016] VDE Verband der Elektrotechnik Elektronik und Informationstechnik e. V.: VDE Trendreport 2016. Internet der Dinge - Industrie 4.0. http://info.vde.com/goto.php?l=dq8zol.1q7d72d,u=989bcd3af624fa771465a57cdc9eec63,n=98ibt.15cmlin,art_id=98ibu.1t5icbp.

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 ● 76131 Karlsruhe ● Germany
Phone +49 721 96 58 590 • Fax +49 721 96 58 589
E-mail info@profibus.com
www.profibus.com ● www.profinet.com