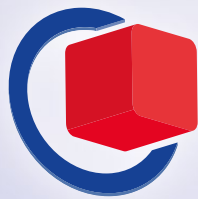


Nuremberg, Germany
14.–16.3.2023



embeddedworld

Exhibition & Conference

... it's a smarter world

CONFERENCE PROCEEDINGS

www.embedded-world.eu

Organized by

**DESIGN &
ELEKTRONIK**
KNOW-HOW FÜR ENTWICKLER

NÜRNBERG MESSE

Conference Sponsors



embedded world Conference 2023

ISBN 978-3-645-50197-2

Conference Chair:

Prof. Dr.-Ing. Axel Sikora, Hochschule Offenburg / Hahn-Schickard-Gesellschaft

Steering Board:

Prof. Dr.-Ing. Peter Fromm, Hochschule Darmstadt

Dr.-Ing. Bernd Hense

Joachim Kroll, Editor-in-Chief DESIGN&ELEKTRONIK

Prof. Dr. Dirk Pesch, University College Cork

Copyright

©2023 WEKA FACHMEDIEN GmbH, Richard-Reitzner-Allee 2, 85540 Haar, Germany,
phone: + 49. (0) 89.255 56 – 1000, e-mail: info@weka-fachmedien.de

This special publication is licensed under CC BY 4.0.

You are free to:

Share – copy and redistribute the material in any medium or format.

Adapt – remix, transform, and build upon the material for any purpose, even commercially.

The publisher, his employees and agents exercise the customary degree of care in accepting and checking conference papers, but are not liable for misleading or deceiving conduct by the client.

embedded world Conference 2023 **embedded.responsible.sustainable**

Welcome to the 21st edition of embedded world Exhibition & Conference held in Nuremberg in March 2023! The **unique combination** of an exhibition for engineers and technical management and a world-leading conference at the intersection of applied research and industrial applications has proven extremely successful. embedded world is **driven by technology** as well as by applications with a strong focus on **system and cross domain aspects**.

In the embedded world, we see three mega-trends that are defining the slogan of this year's edition:

embedded: We are seeing an ongoing use of embedded systems in all smart and connected applications. The complexity of dependable electronic and software systems is ever increasing considering aspects such as reliability and resilience, safety and security, embedded software architectures and hardware-software-co-design, RTOS integration and virtualization, value, production and supply chains, and many many more.

responsible: With the continuous increase of complexity we are reaching new levels of dependability of embedded systems. Already today many systems are so complex and have so many subsystems that individual stakeholders are not any longer able to grasp the complexity of the overall system.

Also, embedded systems can be used for beneficial purpose – like sustainability, but also for malicious applications around societal and political supervision, criminal applications, and alike. We feel that the embedded community should be held responsible for these applications

sustainable: Sustainability is another mega-trend with two facets for the embedded world:

Embedded systems are a cornerstone for making their host systems efficient and sustainable. Think of efficient combustion engines, of electric cars, of smart grids, of home automation, of all these thousands of smart systems

On the other side, we need to think about how to make embedded systems sustainable. This does not only include clean and efficient production with minimum shipment, but also updatibility, repairability, and energy autonomy.

The 21st edition of the embedded world delivers a thrilling programme **structured along 9 tracks**. The programme features a total duration of **200 nonstop hours** of knowledge delivery and exchange.

• All **65 sessions** will not only include **195 presentations**, but also **offer Q&A rounds** in each session amongst speakers and participants.



Prof. Dr.-Ing. Axel Sikora
Chairman of embedded world Conference

• We will have **three first-class keynotes** from top notch industry and academic leaders, including

On Tuesday, Daniel Cooley, CTO of Silicon Labs, will talk on *"Charting the Connected Future"*.

Wednesday will see a keynote by Prof. Hessami, Chair IEEE P7000 Technology Ethics Standard committee, on ethical and responsibility engineering

Prof. Dr. Albert Heuberger, director of the renowned Fraunhofer IIS institute, will deliver a keynote on *"Chip Design and Production: Perspectives and role in Europe's Competitiveness"* on Thursday.

• **18 half- or full day classes** will enable an in-depth knowledge transfer of relevant and actual embedded systems topics.

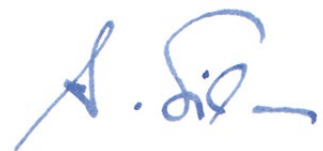
• We will also feature **six plenary panel discussions** not only on hot technological topics, like embedded vision, but also about societal aspects such as "Sustainability and IoT", "Responsible AI", "EU Cyber Resilience Act", and "Supply Chain Challenges".

Let me also highlight the positive and fruitful collaboration with a range of communities, alliances, and interest groups. We organized and are running special sessions with alliances such as the Bluetooth SIG, HiPEAC, MIPI Alliance, MISRA, OSADL, or the RISC-V Foundation. This makes the embedded world truly a **community of communities**. We are grateful for this collaboration.

embedded world 2023 will cover all aspects of the development and application of embedded systems, from fundamental technologies to development processes and special fields of applications. It is one of the central strengths of the event to be cross-sectoral and interdisciplinary. The conference provides a platform to bring together experts from different domains and application areas of embedded systems in order to promote a holistic system design perspective, to identify synergies and commonalities, and to strengthen the exchange of knowledge and experience.

The steering board of embedded world 2023 wishes all participants stimulating discussions about new ideas and solutions enabling the community to more easily and efficiently cope with the immense challenges that lie ahead for our industry and society. We welcome you to gain great insights in a pulsating atmosphere.

Best regards & stay safe!



Prof. Dr.-Ing. Axel Sikora
Chairman of embedded world Conference

Security Extensions for PROFINET

Concepts, Status, and Prospects

Prof. Dr.-Ing. Karl-Heinz Niemann

Institute for Sensor Technology and Automation
Hannover University of Applied Sciences and Arts
Hannover, Germany
karl-heinz.niemann@hs-hannover.de

Andreas Walz, Prof. Dr.-Ing. Axel Sikora

Institute of Reliable Embedded Systems and
Communication Electronics (ivESK)
Offenburg University of Applied Sciences and Arts
Offenburg, Germany
{andreas.walz, axel.sikora}@hs-offenburg.de

Abstract— Operators of production plants are increasingly emphasizing secure communication, including real-time communication, such as PROFINET, within their control systems. This trend is further advanced by standards like IEC 62443, which demand the protection of realtime communication in the field. PROFIBUS and PROFINET International (PI) is working on the specification of the security extensions for PROFINET (“PROFINET Security”), which shall fulfill the requirements of secure communication in the field.

This paper discusses the matter in three parts. First, the roles and responsibilities of the plant owner, the system integrator, and the component provider regarding security, and the basics of the IEC 62443 will be described. Second, a conceptual overview of PROFINET Security, as well as a status update about the PI specification work will be given. Third, the article will describe how PROFINET Security can contribute to the defense-in-depth approach, and what the expected operating environment is. We will evaluate how PROFINET Security contributes to fulfilling the IEC 62443-4-2 standard for automation components.

Two of the authors are members of the PI Working Group CB/PG10 Security.

Keywords—industrial security; PROFINET

I. INTRODUCTION (*Heading 1*)

Ethernet-based realtime communication, like PROFINET, is becoming gradually prevalent in the automation domain and replaces fieldbus technology. In factory automation, realtime Ethernet is standard since many years. The process industry is catching up and increasingly uses realtime Ethernet like PROFINET in chemical plants, the pharmaceutical industry, water and waste water and other applications [1]. With the use of two-wire Ethernet even the communication with single sensors via Ethernet (Ethernet APL) [2] is possible. The use of a single, converged network enables many other use cases, like direct access to sensors for computerized maintenance systems (CMMS). These new integration features demand improved security features of the underlying communication protocol.

PROFINET got developed in the 1990s. At this point in time, IT Security for production systems (here called OT security) was not an issue. The main protective measure was the separation of the OT network from the IT network, also known as “cell protection”. With the increasing integration of applications in the context of industry 4.0 and the increasing number of cyber-attacks in the automation domain [3–5], the protection of realtime communication protocols in the OT domain is key.

PROFIBUS and PROFINET International (PI) works on security extensions for PROFINET to provide cryptographic protection of PROFINET protocol exchanges, including realtime communication. This paper will provide an overview of the security extensions for PROFINET, which shall be referred to as “PROFINET Security” in the following. It reflects the activities of the working group CB/PG10 (“Security”) within PI.

The work presented herein is the result of concerted effort of many experts and not just the authors of this article. The authors would like to thank all involved persons for the fruitful and inspiring cooperation and the valuable contributions.

One of the main objectives of PROFINET Security is to provide technical measures to address the security requirements laid out by IEC 62443, a series of standards focused on OT security. Therefore, the main part of our article starts with an overview of IEC 62443 (Chapter II). It is followed by a conceptual overview of PROFINET Security (Chapter III). Chapter IV discussed how PROFINET Security can act as a building block to implement secure industrial automation in accordance with IEC 62443. Finally, Chapter V provides a summary and concludes with an outlook.

II. IEC 62443 OVERVIEW

The IEC 62443 series of standards focuses on OT security. In the final expansion it will consist of 15 parts, of which two are the most relevant for manufacturers.

- Part IEC 62443-4-1 [6] defines a secure development workflow. It describes the organizational and procedural

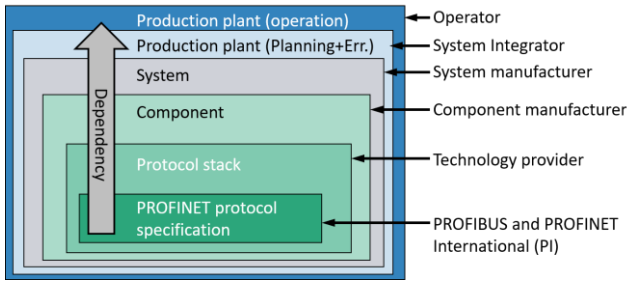


Figure 1: Roles in the security process [8]

measures that a manufacturer of automation components and systems has to observe, which encompass, among other things: training of the staff, risk analysis, security specification, security implementation, security test, user documentation.

- Part IEC 62443-4-2 [7] defines the security specific requirements for components, such as: user authentication, secure communication, software integrity, integrity of software updates, event logging and much more.

The IEC 62443 series of standards defines different roles in the security process. Figure 1 maps these roles to the different building blocks of an automation system and the respective stakeholder.

The PROFINET protocol specification constitutes the fundament of the security process. On this basis the other stakeholders build the protocol stacks, the components and the systems. Each of these stakeholders has its own responsibility in this process, which goes beyond the pure view on the communication. The following chapters will focus on PROFINET Security, which is the basis for secure realtime communication in the field with PROFINET. Further Information can be found in [8].

III. PROFINET SECURITY: CONCEPTUAL OVERVIEW

In the following, we provide a conceptual overview of PROFINET Security as defined and specified by PI [9–11].

A. PROFINET Security Classes and Secure Application Relations

With PROFINET Security, three so-called Security Classes are defined, called Security Classes 1, 2 and 3. Security classes classify PROFINET component and tool capabilities. Higher security classes comprise the capabilities of lower security classes.

Compared to classical PROFINET, Security Class 1 introduces improved configuration capabilities for network management (SNMP) and device discovery and configuration (DCP) protocols. Additionally, it introduces a mechanism for PROFINET component manufacturers to cryptographically sign device description (GSD) files. Its use is mandatory for Security Class 1 components. However, Security Class 1 does not introduce any cryptographic mechanisms for protecting PROFINET protocol exchanges. A summary of Security Class

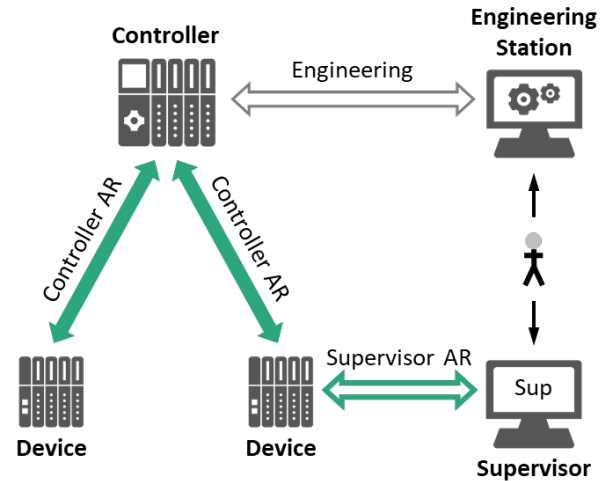


Figure 2: PROFINET application relations [11]

1 features can be found in a dedicated PI Guideline [12]. We will focus on Security Classes 2 and 3 in the following.

The major novelty introduced with Security Classes 2 and 3 is the option for built-in cryptographic protection of PROFINET protocol exchanges. Between PROFINET components supporting at least Security Class 2, so-called Secure Application Relations (secure ARs) can be established.

Figure 2 illustrates the PROFINET Application Relations (AR) that Security Classes 2 and 3 allow to turn into secure ARs: these are the so-called Controller ARs between a Controller and a Devices (e.g. remote IOs) as well as so-called Supervisor ARs between a Supervisor and a Device. The following chapters will focus on the application relations in Figure 2 marked in green.

Secure ARs differ from classical (plain) PROFINET ARs mainly in the following ways:

- The two involved PROFINET endpoints must mutually authenticate using public-key certificates before relevant PROFINET communication may occur within the secure AR.
- Traffic of all Communication Relations (CRs) occurring under the umbrella of the secure AR is protected using state-of-the-art symmetric cryptography.
- The invocation of operations and services through the secure AR can be protected by role-based access control mechanisms.

An illustration of a secure AR is provided in Figure 3.

Note that PROFINET Security does not cover non-PROFINET interfaces. In particular, communication between an engineering station and a Controller, just as authentication of human users is out-of-scope for PROFINET Security. The respective manufacturer is responsible for addressing related security requirements.

The cryptographic mechanisms offered by Security Classes 2 and 3 cover integrity protection and confidentiality for acyclic

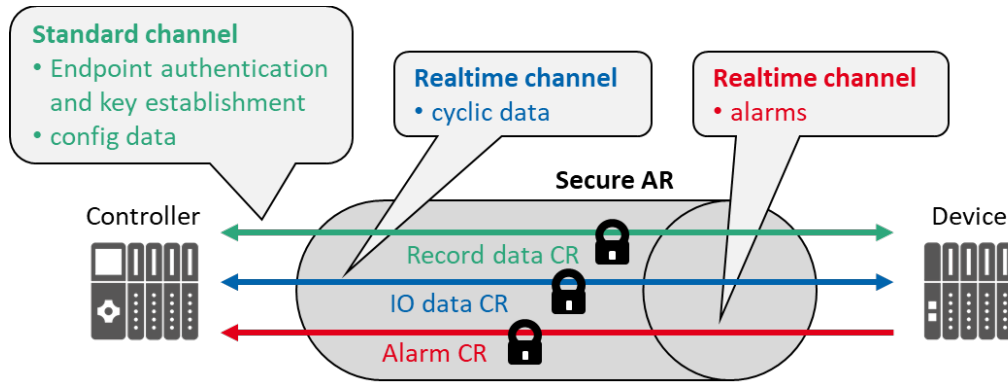


Figure 3: PROFINET secure application relation. Just like for plain ARs, a secure AR comprises multiple CRs. Each CR inside a secure AR is cryptographically protected using symmetric cryptography. Certificate-based endpoint authentication and cryptographic key establishment is integrated into the Record data CR.

TABLE I. SECURITY FUNCTIONS SUPPORTED BY PROFINET SECURITY (M: mandatory, -: not supported, \checkmark : enabled by default)

Highest mutually supported Security Class	GSD	Record data CRs		IO data CRs		Alarm CRs	
	Integrity protection	Integrity protection	Confidentiality	Integrity protection	Confidentiality	Integrity protection	Confidentiality
1	M	-	-	-	-	-	-
2	M	\checkmark	\checkmark	\checkmark	-	\checkmark	??
3	M	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark

communication (i.e., Record data and Alarm CRs), and integrity protection for cyclic realtime communication (i.e., IO data CRs). The key difference between Security Classes 2 and 3 is that Security Class 3 additionally offers confidentiality for cyclic realtime communication. Table 1 summarizes the cryptographic features of Security Classes 1 to 3.

While integrity protection is always enabled for all CRs within a secure AR, confidentiality may be enabled or disabled for CRs individually. The owner/operator actively needs to disable confidentiality during engineering, if it is supported but not desired. Reasons to do so may be the need to enable on-the-wire diagnosis or simply performance limitations possibly implied by confidentiality.

More generally speaking, enabling certain cryptographic security feature may come with a degradation of the supported cycle time on IO data CRs or the number of secure ARs simultaneously manageable by a Controller. In case of conflicting requirements, careful weighting must be done. In practice, it can be assumed that confidentiality of cyclic IO data is rarely required.

B. Cryptographic Algorithms and Protocols

PROFINET Security resorts to existing security standards and technology as much as technically possible. It uses strong, well-known, and widely accepted cryptographic algorithms and protocols.

PROFINET Security is designed for extensibility and crypto agility: support for new cryptographic algorithms and protocols may be added easily if, for instance, required by national regulations or because today's choices get broken.

PI has carefully selected an initial set of cryptographic algorithms and protocols.

For endpoint authentication and cryptographic key establishment, PROFINET Security uses the Transport Layer Security (TLS) protocol [13] wrapped into the Extensible Authentication Protocol (EAP) protocol [14]. EAP-TLS is part of the IEEE 802.1X standard for Port-Based Network Access Control [15]. The public-key certificates for PROFINET Security are based on the IEEE 802.1AR standard on Secure Device Identity [16], using elliptic curve cryptography (ECC) with curves Curve25519, Curve448, NIST P-256, or NIST P-521.

For integrity protection and confidentiality of communication relations within secure ARs, the Advanced Encryption Standard (AES) with 256-bit keys in Galois Counter Mode (GCM) is used. AES-GCM is a member of the Authenticated Encryption with Associated Data (AEAD) class of algorithms [17]. It can be operated in both integrity-and-confidentiality as well as integrity-only mode.

Note that, while PROFINET Security relies on the TLS protocol as described above, it does so only for endpoint authentication and cryptographic key establishment. This is a property intentionally inherited from the EAP-TLS protocol, which is mainly driven by the handshake layer of TLS. For bulk data exchanges occurring within the CRs of secure ARs, PROFINET Security uses an approach that is similar, yet not identical, to the record layer of TLS.

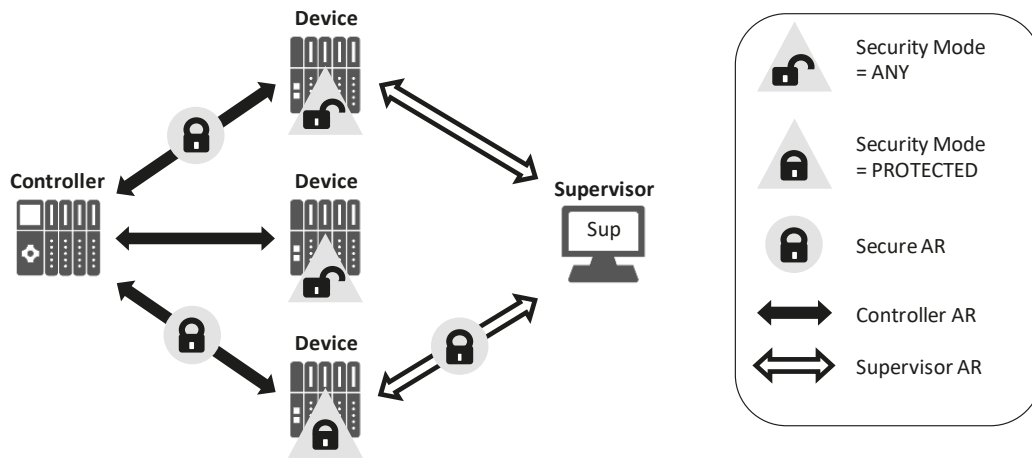


Figure 4: Coexistence example of secure and plain ARs. The figure shows a simple PROFINET IO system with one Controller and three Devices. An optional Supervisor entity is also present. The Controller maintains secure and plain ARs to different Devices in parallel. The Supervisor establishes secure and plain ARs to some Devices one after the other. A Device with its Security Mode set to "ANY" accepts secure and plain ARs, otherwise only secure ARs.

C. Coexistence of Secure and Plain ARs

Secure ARs and plain ARs (ARs without security functionality) can coexist without interference. This holds true within a single network, within a single PROFINET IO system, and at a single PROFINET endpoint.

To prevent a PROFINET component from unintentionally accepting plain AR establishment requests, a security configuration parameter, called Security Mode, is introduced. The Security Mode is a binary and persistent parameter (= ANY or PROTECTED), which exists once for each PROFINET component that supports Security Class 2 or 3. If set to PROTECTED, the component will accept incoming ARs only if they are secure ARs. It is the owner's/operator's responsibility to set the Security Mode of components appropriately. Setting its value is subject to authorization as provided within secure ARs.

Figure 4 provides an example of the coexistence of secure and plain ARs.

D. Security Configuration and Certificate Management

In order to allow for secure PROFINET communication among the components of a PROFINET IO system, a coordinated management of security configurations, public-key certificates, keys, and trust anchors is necessary.

Note that, in the following, we use the term "certificate" as a synonym for "public-key certificate". It is not to be confused with a certification of product compliance.

PROFINET Security Configuration Management (SCM), introduced with PROFINET Security Classes 2 and 3, denotes protocol extensions to PROFINET that facilitate such management. A new functional role, called Security Infrastructure Handler (SIH), is responsible to initiate and orchestrate corresponding PROFINET SCM protocol exchanges with PROFINET components. In this course, their security configurations, certificates, keys, and trust anchors can be

supplied, refreshed, removed, or invalidated. The SIH role is going to physically coincide with a PROFINET Controller in most cases, but engineering and diagnosis tools are possible hosts, too.

The certificates ("LDevIDs" in terms of IEEE 802.1AR) that PROFINET components use to authenticate each other are specific to the particular owner/operator. That is, no such certificates are available on PROFINET components in factory default state. Therefore, it is the owner/operator's responsibility to issue, distribute, and manage these certificates, using the technical provisions provided by the SIH role/tool.

PROFINET Security supports using certificates issued to components by their manufacturers ("IDevIDs" in terms of IEEE 802.1AR) for an initial security setup. Manufacturers can ship their components with such IDevID certificates, independent of PROFINET and PROFINET Security. IDevIDs

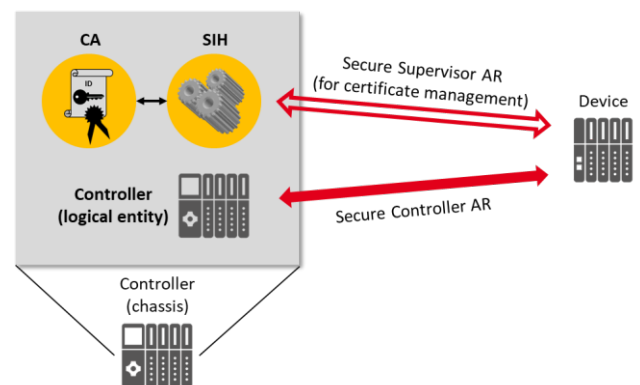


Figure 5: Possible integration of an SIH and a CA in a PROFINET Controller chassis. The combination of CA and SIH located inside a physical Controller allows for seamless certificate, key, and trust anchor management on related Devices.

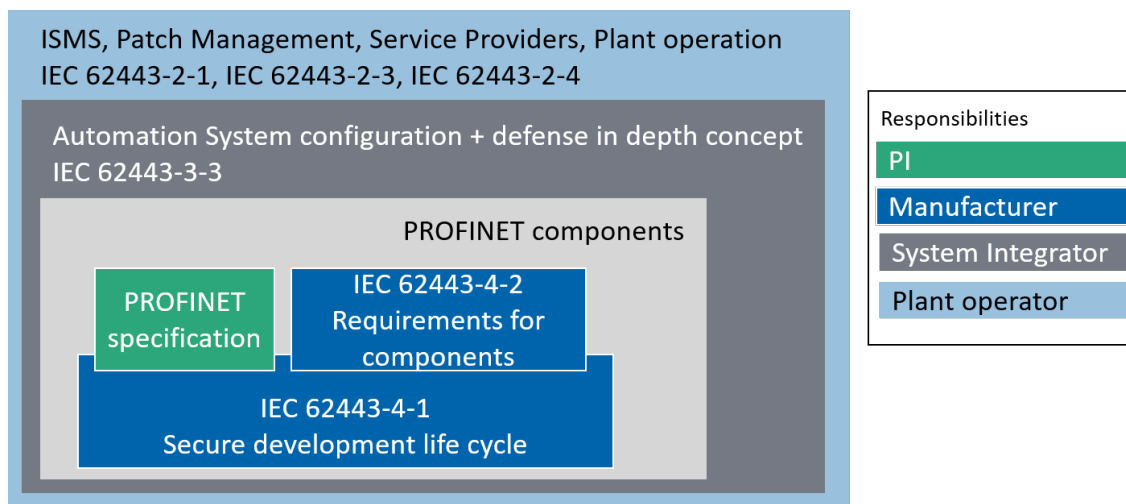


Figure 6: Building blocks for a secure production system

enable a cryptographic verification of the identity and origin claims of a component over the network. Using such certificates for protecting operational PROFINET communication is not supported by PROFINET Security, though.

As illustrated in Figure 5, an SIH can be joined with an integrated Certificate Authority (CA) functionality. Alternatively, it may also resort to external (e.g., on-premise or third-party) CA services. A Controller with SIH role and integrated CA functionality can enable a fully automated certificate management for PROFINET components within its PROFINET IO system. This includes, for example, one of the most challenging use cases: a fully automated and instantaneous certificate handling when a faulty PROFINET component unexpectedly needs to be replaced by a new one.

IV. PROFINET SECURITY AS BUILDING BLOCK FOR SECURE INDUSTRIAL AUTOMATION

The PROFINET Security concept is one of the cornerstones to fulfill one of the key requirements of the IEC 62443-4-2 [7]. Chapter 7.3.1 of this standard defines that "[t]he automation system must have the capability to protect the integrity of the transmitted information". This integrity protection will be possible by using the PROFINET protocol with the described extension. However, integrity protection is only one of the building blocks for a secured automation system.

Figure 6 shows the building blocks for a secure production system, from the IEC 62443 perspective. The PROFINET Specification [9, 10], constituting the foundation of a PROFINET component, and includes the security extensions described in Chapter 3. On this basis, component and automation system manufacturers can develop PROFINET components. These components, in turn, are subject to the security requirements of the IEC 62443-4-2 [7]. IEC 62443 imposes a number of requirements, some of which can directly be addressed by PROFINET Security. This includes the integrity protection and optional confidentiality of PROFINET communication. Further requirements need to be fulfilled by the component and/or system manufacturer. For instance, the R&D

organization of the manufacturers needs to work according to the secure development lifecycle according to IEC 62443-4-1 [6].

A system integrator can design an automation system, based on the components. The security requirements to be observed during this planning process are described in IEC 62443-3-3 [19]. This work includes, for example, the implementation of a defense in depth approach, the implementation of access control, the separation of the OT network and much more.

After the commissioning phase, the plant owner/operator assumes control of the system. During the operation phase, security relevant tasks need to be processed. The plant operator needs to implement an Information Security Management System (ISMS). Such an ISMS can be either implemented according to the ISO 27001 standard [20] or according to the IEC 62443-2-1 [21]. Guidance to use which of the two standards can be found in [22].

In addition, the plant operator needs to take care of the patch management of the system (see IEC TR 62443-2-3 [23]) and the secure handling of service providers according to IEC 62443-2-4 [24].

V. SUMMARY, CONCLUSION AND OUTLOOK

With PROFINET Security, an integration of cryptographic protection into the PROFINET protocol has been achieved. It constitutes an important step towards secure communication within PROFINET-powered automation systems. In this article, we presented a high-level overview of the technical concept behind PROFINET Security. Additionally, we sketched how PROFINET Security can help to address requirements imposed by IEC 62443.

The concepts behind PROFINET Security are coined by the demand to minimize disruption of PROFINET features as known and appreciated by its wide user base today. Many technical and integration challenges had to be solved on the way. As a result, PROFINET Security promises to harmonize ecosystem, automation, and security requirements in an effective way.

Currently, the process of integrating PROFINET Security into the specification is in progress. In parallel, the transfer into the IEC standard IEC 61158-5-10 [25] and IEC 61158-6-10 [26] is ongoing. In a next step, PROFINET Protocol stacks need to be updated to incorporate PROFINET Security features. This will then serve as input to PROFINET components and systems.

PI strives to achieve a pre-certification of PROFINET Security in accordance with IEC 62443-4-2 [7]. This shall support component manufacturers in their own IEC 62443 certification process.

ACKNOWLEDGMENT

The work presented herein is the result of concerted effort of many experts and not just the authors of this article. The authors would like to thank all involved persons for the fruitful and inspiring cooperation and the valuable contributions.

REFERENCES

- [1] PROFIBUS Nutzerorganisation e.V. "PROFINET - The Solution Platform for Process Automation." https://www.profibus.com/index.php?eID=dumpFile&t=f&f=133940&t_oken=60acf6a7451d29bcf233633412d644d58f109bbb
- [2] PROFIBUS and PROFINET International, Fieldcom Group, OPC- Foundation, and ODVA Inc. "Ethernet to the field: White Paper." <https://www.profibus.com/download/apl-white-paper>
- [3] Claroty Ltd. "The Global State of Industrial Cybersecurity 2021: Resilience amid Disruptions." https://claroty.com/wp-content/uploads/2022/02/Claroty_Report_State_of_Industrial_Cybersecurity_2021.pdf
- [4] Dragos Inc. "ICS/OT Cybersecurity: Year in review 2021." <https://hub.dragos.com/hubfs/333%20Year%20in%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20in%20Review%20-%20Dragos%202021.pdf?hsLang=en>
- [5] Fortinet inc. "2022 State of Operational Technology and Cybersecurity Report." <https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf>
- [6] Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements, IEC 62443-4-1, IEC- International Electrotechnical Commission, Jan. 2018.
- [7] Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components, IEC 62443-4-2, IEC- International Electrotechnical Commission, Feb. 2019.
- [8] PROFIBUS Nutzerorganisation e.V. "OT security for production plants with PROFINET: A classification of IEC 62443 for operators, integrators and manufacturers." <https://www.profibus.com/download/white-paper-ot-security-classification-of-iec62443>
- [9] PROFIBUS Nutzerorganisation e.V. "Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO: Version 2.4 MU3." <https://www.profibus.com/download/profinet-specification>
- [10] PROFIBUS Nutzerorganisation e.V. "Application Layer services for decentralized periphery: Technical Specification for PROFINET IO, Version 2.4 MU3 – Oct. 2021." <https://de.profibus.com/downloads/profinet-specification/>
- [11] PROFIBUS Nutzerorganisation e.V. "Security Extensions for PROFINET - PI White Paper for PROFINET." <https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/> (accessed Sep. 7, 2019).
- [12] PROFIBUS Nutzerorganisation e.V. "Security Class 1 for PROFINET- Security." <https://www.profibus.com/download/profinet-security-guideline>
- [13] Network Working Group. "The Transport Layer Security (TLS) Protocol: RFC 5246." <https://www.ietf.org/rfc/rfc5246.txt>
- [14] Network Working Group. "The EAP-TLS Authentication Protocol: RFC 5216." <https://www.rfc-editor.org/rfc/pdf/rfc5216.txt.pdf>
- [15] Network Working Group. "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) - Usage Guidelines." <https://www.rfc-editor.org/rfc/pdf/rfc3580.txt.pdf>
- [16] IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity, IEEE 802.1AR-2018, IEEE Computer Society. [Online]. Available: <https://1.ieee802.org/security/802-1ar/>
- [17] Network Working Group. "An Interface and Algorithms for Authenticated Encryption: RFC 5116." <https://www.rfc-editor.org/rfc/pdf/rfc5116.txt.pdf>
- [18] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, Network Working Group IETF, May. 2008. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5280>
- [19] Security for industrial automation and control systems Part 3-3: System security requirements and security levels, IEC 62443-3-3:2013, IEC- International Electrotechnical Commission, Jun. 2013.
- [20] Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO/IEC 27001:2022, International Organization for Standardization (ISO), Oct. 2022. [Online]. Available: <https://www.iso.org/standard/82875.html>
- [21] Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, IEC 62443-2-1-2010, IEC- International Electrotechnical Commission, Nov. 2010. [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx
- [22] K.-H. Niemann. "Differentiation of the IT security standard series ISO 27000 and IEC 62443: Whitepaper." https://library.e.abb.com/public/fc76636ebcd845b88c640a613f0c95a0/3ADR010839_Differentiation_ISO_27001_IEC_62443_REV_C_en_US.pdf
- [23] Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment: Technical Report, IEC TR 62443-2-3, IEC- International Electrotechnical Commission, Jun. 2015. [Online]. Available: <https://www.vde-verlag.de/iec-normen/221941/iec-tr-62443-2-3-2015.html>
- [24] Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers, IEC 62443-2-4:2015+AMD1:2017 CSV consolidated version, IEC- International Electrotechnical Commission, Aug. 2017.
- [25] Industrial communication networks - Fieldbus specifications - Part 5-10: Application layer service definition - Type 10 elements, IEC 61158-5-10:2019, IEC- International Electrotechnical Commission, 2019. [Online]. Available: <https://webstore.iec.ch/publication/64836>
- [26] Industrial communication networks - Fieldbus specifications - Part 6-10: Application layer protocol specification - Type 10 elements, IEC 61158-6-10:2019, IEC- International Electrotechnical Commission, 2019. [Online]. Available: <https://webstore.iec.ch/publication/59893>

Contact

Project Manager:

Renate Ester
P + 49 (0)89 255 56-1349
E-Mail: REster@weka-fachmedien.de

Coordinator Conference Attendees:

Alexandra Feuerstein
P + 49 (0)89 255 56-1372
E-Mail: AFeuerstein@weka-fachmedien.de

WEKA FACHMEDIEN GmbH
Richard-Reitzner-Allee 2
85540 Haar, Germany
www.weka-fachmedien.de

