IT security extensions for PROFINET

Karl-Heinz Niemann
Faculty I – Electrical Engineering and Information Technology
Hochschule Hannover - University of Applied Sciences and Arts
Hannover, Germany
Karl-Heinz.Niemann@Hs-Hannover.de

***Abstract*—The impact of vertical and horizontal integration in the context of Industry 4.0 requires new concepts for the security of industrial Ethernet protocols. The defense in depth concept, basing on the combination of several measures, especially separation and segmentation, needs to be complimented by integrated protection measures for industrial real-time protocols. To cover this challenge, existing protocols need to be equipped with additional functionality to ensure the integrity and availability of the network communication, even in environments, where possible attackers can be present. In order to show a possible way to upgrade an existing protocol, this paper describes a security concept for the industrial Ethernet protocol PROFINET.**

PROFINET security, cyber security, IT security, protocol extensions

I. Current State of Technology

Ethernet-based communication in the production domain gains more and more importance. According to [1] Ethernet based automation networks reached in 2018 a market share of 51% worldwide. Along with this increased use, the structure of automation networks changes.

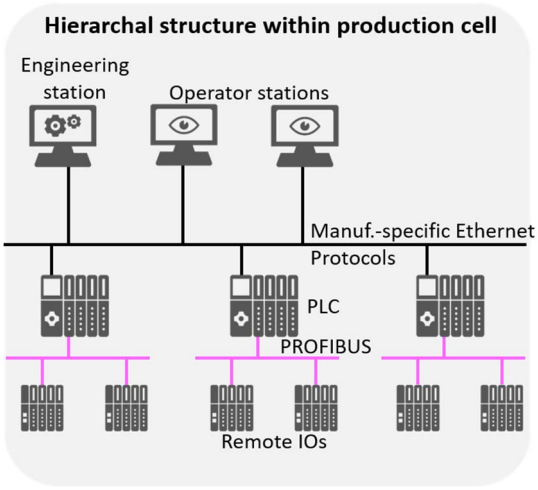

Fig. 1. Traditional automation system structure

Fig. 1 shows a production cell with a traditional, hierarchical automation system structure with a staged network. The industrial Ethernet connects operator and engineering stations with the PLCs. A fieldbus (e. g. PROFIBUS) connects the Remote IOs to the PLCs.

Fig. 2 shows the system structure of a production cell with a uniform communication network. A single Ethernet network, in this case PROFINET, interconnects all components of the automation system. A number of such cells is used for a plant. The cells have connection to a superordinate level, usually via router and firewall. Simple field devices will be connected in future directly to the network, for example via IEEE 802.3cg single pair Ethernet [2] [3]. The flat network structure yields benefit with respect to the vertical integration of the plant, allows direct access to all components of the automation system and eases the network management.

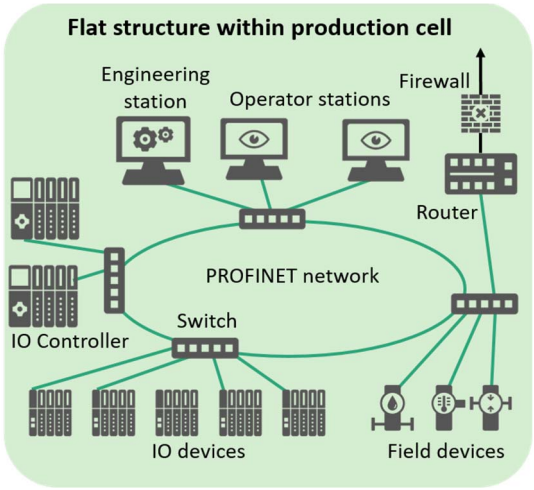

Fig. 2. Flat system structure

Besides the described advantages, the uniform structure implies risks with respect to IT security. This network architecture allows potential attackers to directly access all devices in the network, using the same network protocol, even though an additional network segmentation is used. Intruders that manage to bypass the firewall or insiders [4] [5] are able to tamper with all devices in the network and cause outages of the control system. This currently applies to all industrial Ethernet protocols, not only to PROFINET.

DOI of the original publication: 10.1109/INDIN41052.2019.8972209

Currently PROFINET uses a defense in depth strategy as described in [6]. This concept relies on a separation of the automation system from the rest of the company's IT infrastructure and a segmentation of the network inside the automation domain in order to restrict the data flow [7]. The recent IT security concept for PROFINET is described in [8]. In addition to the general security concept, security requirements for devices have been defined in [9]. These mainly define robustness requirements for devices in order to handle network overload conditions (denial of service). Briefly: The recent PROFINET security concept relies on the network separation and the robustness of the components.

As the recent security concept does not provide any means of protection against cyber-attacks, the integrity, authenticity and availability of the automation system are at risk, in case intruders manage to directly access the automation network. In [10] a man in the middle attack against PROFINET is described. The source [11] shows that replay attacks against PROFINET are possible. The possible attack vector from the outside can be mitigated, by using a network segmentation in combination with a demilitarized zone [12] or by an intrusion detection system. In [13] the authors evaluate the use of such a system in a PROFINET environment.

Even though the described measure improve the situation, industry users like the User Association of Automation Technology in Process Industries (NAMUR) demand an integrated approach, where the communication is protected by integrated means in the devices (security by design) and not by a separation of the networks only [14]. This implies cryptographic measures will be needed to protect the network communication.

Several research projects evaluated the feasibility of security functions inside the PROFINET protocol. In [15] a security layer on top of the PROFINET application layer is proposed. This security layer is described as comparable to the PROFIsafe communication profile. The approach shall avoid any changes to the existing protocol stacks. The research project "SEC_PRO" evaluated a security layer for PROFINET above the data link layer [16]. The project [17] evaluated different MAC algorithms and their performance. In [18, 19] the authors evaluate PROFINET in combination with transport layer security. The recent publications show that different approaches are possible to protect the PROFINET communication.

Other Organizations dealing with Industrial Ethernet Protocols work on comparable solutions to increase the security of their networks. The ODVA describes in [20] the needed measures to increase the security of Ethernet IP Networks. Also, in building automation security extensions, Ethernet based communication protocols, like BACNET are in place [21].

II. Requirements for PROFINET Security

Even though several proposals for a security layer are available, PROFIBUS and PROFINET International (PI) decided, to set up the working group PG/WG10 Security in order to find a solution that meets the needs of the users and vendors. The following chapters describe the concept developed in this working group so far.

In a first step, a STRIDE analysis according to [22] was performed in order to identify the recent security status of the PROFINET protocol through the analysis of attack scenarios. Base on that work, the WG defined security objectives and their importance for PROFINET.

TABLE I. Generic Security Objectives For Profinet

Security objective	***Priority and Relevance for PROFINET***
Integrity	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	Low: The security objective "confidentiality of IO data" is estimated as low, as long as no conclusions can be drawn from the IO data with regard to company secrets (e.g., recipes).
Availability	High: Depending on the production process, there are generally high to very high availability requirements. This is especially true for critical infrastructures.
Authenticity	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 identity.
Authorization	High: The usage control ensures that only authorized users can intervene in the automation system.
Non-repudiation	Medium: Refers to installations where traceability of user intervention is required. For example, in pharmaceutical plants operated in accordance with FDA 21 CFR Part 11 [23]

Table 1 shows that all objectives, except authenticity and non-repudiation are valued "high". Section III will show that a scalable approach will meet these requirements. In order to fulfill the security objectives, a joint effort of manufacturers, system integrators and plant operators will be necessary.

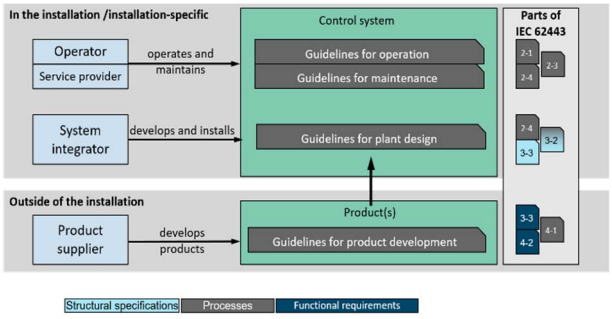

Fig. 3. Stakeholders in the security process according IEC 62443-2-2 [24]

Fig. 3 shows the interaction of the stakeholders according to [24]. The functional requirements for product development have to be derived from [7] and [25]. The focus for this paper will be on the product suppliers. In order to identify the objectives related to the protocol, the working group decided to define tasks for the product suppliers and PI according to Fig. 4.

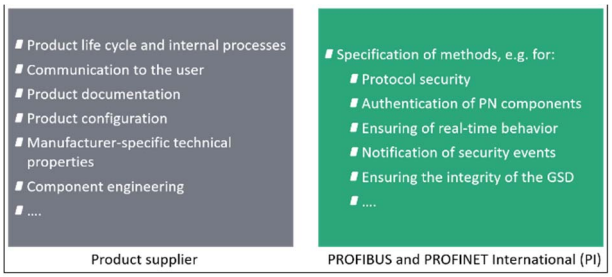

Fig. 4. Differentiation security related tasks between product supplier and PI

The rest of the paper will now focus on the protocol extensions shown in the right column of Fig. 4. In a next step, the PROFINET specific security objectives, allocated to operation phases, were defined according to Table II. The phases can be described as follows: Engineering is the phase where the control system is engineered. This phase is mainly executed on the engineering station, followed by the download of the data to the controllers. Startup describes the establishment of the communication relations. Operation is the phase after the establishment of the communication relations. During this phase, the cyclic transfer of the IO data takes place. Maintenance describes a phase where SW updates and other maintenance work is performed. These phases reflect the "normal" behavior of the automation components. The additional security features shall not change this behavior.

TABLE II. SPECIFIC SECURITY OBJECTIVES FOR PROFINET

Phase	***Generic Objective***	***Specific objective***
Ope-ration	Integrity	User specified operation must not be changed
	Integrity Authenticity Authorization	Prevent unauthorized access of IO supervisor or tampering with the data transferred by the IO supervisor..
	Integrity	Clock and IRT Clock synchronization
	Availability	Availability of Application Relations (ARs) to be ensured
	Availability	Redundancy function to be ensured
	Confidentiality	Cyclic and acyclic IO data, device module identification, network topology (low priority)
	Availability Confidentiality Integrity	Diagnostic data via SNMP
Startup	Integrity	Ensure integrity of PROFINET device identity
	Integrity	Configuration data
	Integrity	IP and PROFINET network configuration.
	Availability	Established communication relation following a power failure.
	Confidentiality	Configuration data (medium priority).
n.a.	Authenticity	An IO device must not be controlled by an IO controller, other than intended in the planning.
n.a.	Confidentiality	The confidentiality of private keys has to be ensured when using cryptographic processes.
Engineer-ing	Integrity	The integrity and authenticity of the data in the generic station description file (GSD file) have to be ensured.
Mainte-nance	Integrity	The integrity of the firmware in an IO controller and IO device is to be ensured

Besides the functional requirements described above, further requirements that cannot be allocated to an operating phase have to be observed. These are:

- Real-time behavior must be ensured in the presence of security measures.
- Security measures must be state-of-the-art and updateable via software update.
- The use of security measures should follow economic considerations.
- The coexistence of PROFINET components with and without security measures must be possible. Yet, attackers must not be able to force the system into an unsecured operation.
- Exchange of components during runtime must be possible without considerable effort.
- Existing PROFINET profiles such as PROFIsafe must be useable without restriction.
- The solution should be scalable.
- The installed base must be considered.

III. BASIC CONCEPT

Based on the requirements defined in section II the working group defined a basic security concept.

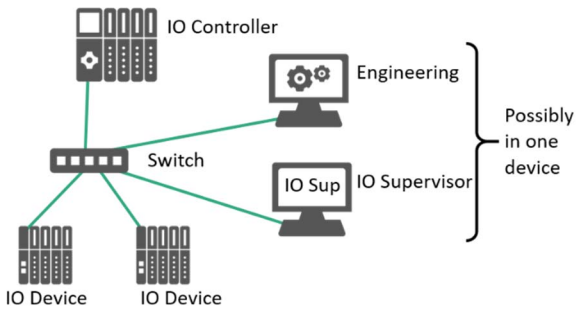

Fig. 5. PROFINET example system (physical view)

Fig. 5 shows the considered example system, used as a basis for the definition of the security concept. The system consists of IO controller, IO devices and a switch. The engineering station and the IO supervisor (additional tool for commissioning and diagnosis) either can be separate tools or unified in one tool.

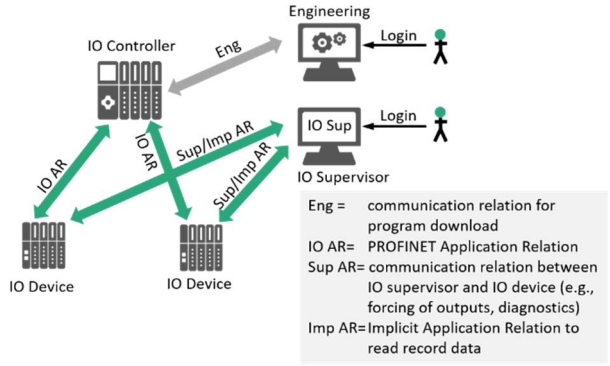

Fig. 6. Application relations in example system (logical view)

Fig. 6 shows the application relations of the sample system. There are IO ARs for the communication between the IO controller and the IO devices, the Supervisor and implicit (Imp) ARs for the communication of the IO supervisor with the IO devices and the Engineering AR for the communication between the engineering station and the IO controller. The PROFINET security concept will consider all ARs marked green. The AR in grey color will be in the responsibility of the product suppliers. All components of the ARs (cyclic data, acyclic data, alarms, etc.) need to be secured by respective security measures.

Table I showed that the different requirements are prioritized differently. In order to generate a scalable approach, the working group decided to specify several, scalable security classes shown in Table III.

TABLE III. PROFINET SECURITY CLASSES

Security class and name	***Definition***
Class 1 Robustness	System protected according chapter II 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.
Class 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.
Class 3 Confidentiality	In addition to the requirements of security class 2, the confidentiality of the communication relations is ensured.

The classes have the following characteristics:

- Security class 1 provides protection according the measures described in chapter II plus short-term incremental improvements.
- 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 cannot be monitored as well. This class is used if the operator has higher IT security requirements on the communication via PROFINET.
- 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 should be able to operate on the basis of security classes 1 and 2. Existing applications (brownfields) will be allocated to security class 1. For security class 2, upgraded components will be needed that implement the additional security function. Based on the requirements in Table II and the subsequent additional requirements, the following security measures were identified:

- The authenticity of PROFINET nodes is ensured through a cryptographically secured digital ID, e.g. in the form of certificates. The concept should also include the secure storage of this ID. For further information, see [26, 27].
- The integrity of the communication is ensured 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.
- The system startup and the assignment of components is secured through cryptographic measures. This also applies for a system startup, following a connection interruption or a power outage.
- PROFINET devices can report security-relevant events, e.g., through additional PROFINET IT security alarms.
- The confidentiality of all acyclic data and of the configuration data is part of the concept. Additionally, the confidentiality of cyclic data will be available as optional feature in security class 3. Please note that the computing power for confidential communication (encryption) is significantly higher, compared to an integrity protection through a cryptographic checksum. A performance value comparison can be found in [28] and [17].
- Ensuring the minimum requirements to protect against denial of service attacks. This aspect has already been realized according to [29] 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.
- Protection of the integrity and authenticity of general station description files (GSD).

Further-reaching requirements, e.g. the secure processing of GSDs in an engineering tool, are to be implemented in a manufacturer-specific manner.

It is planned to equip the devices with certificates as shown in Fig. 7.

Fig. 7. Certificate use with manufacturer and operator certificates

Devices can be delivered with manufacturer certificates (shown in red color). The certificate is securely stored in the device. The manufacturer certificate allows the operator to verify the authenticity of the device on arrival or during commissioning of the device as shown in Fig. 8.

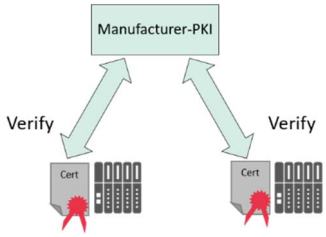

Fig. 8. Verification of manufacturer certificates

This check provides protection against unauthorized reproduction (product piracy). As a next step, the operator adds an operator certificate (shown in green color in Fig. 7), in order to integrate the device to the public key infrastructure (PKI) of the operator.

The system startup is performed in two phases as shown in Fig. 9.

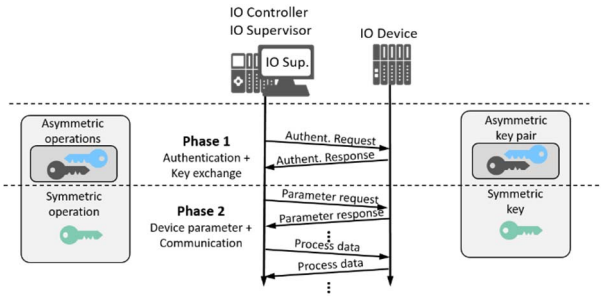

Fig. 9. Two phase system startup

In phase 1, a private/public key process is first used for mutual authentication and to exchange the asymmetric keys between the IO controller or the IO supervisor and the IO device. To do this, the nodes exchange their public keys (blue in Fig. 9). The verification of the keys is performed via the certificates. A secure connection is established. After that the devices negotiate a symmetric key (green in Fig.7) which then is used for the further communication. The changeover to a symmetric key is useful, as the use of symmetric keys demands less computing power than asymmetric keys.

A message authentication code (MAC) protects the PROFINET data packages. The receiver checks the integrity and authenticity of the message through the verification of the checksum. The calculation of the MACs is based on the previously described symmetric keys in combination with a sequence counter. The advantage of this process is the relatively simple calculation of the MAC. In [28] the suitability of various message authentication codes has been evaluated for data packets with a typical length for PROFINET packets. This examination showed that the HMAC-SHA 256 algorithm [30] is the best-performing solution. No final selection of MAC algorithm has been made yet. The hashing-algorithm will be negotiated during the startup process, to allow for a transition to higher-performance algorithms in the future.

The working group decided to build the security concept for PROFINET on a number of building blocks, shown in Table IV.

TABLE IV. BUILDING BLOCK FOR 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-real-time 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	Safeguarding of the connection with respect to configuration tools that access an IO device via a PROFINET read access or by reading and writing of IO parameters, as an IO supervisor does.
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 to ensure the correct implementation of the security measures.
Manufac-turer	Tasks of the manufacturer. These tasks are listed for the sake of completeness but are assigned to the manufacturer.
Documenta tion	Provision of security-relevant information for operators.

Based on these building blocks, a detailed list of needed protocol extensions was generated. See [31] for further details.

IV. CONCLUSION AND NEXT STEPS

The described concept addresses the requirements defined in section II. The intended use of vendor and operator certificates will allow a plant operation without permanent connection to the internet. Pre-studies confirmed that the planned use of hashing algorithms for securing the integrity of the real time packets will suitable to sustain the known real time capabilities of PROFINET in combination with securing mechanisms.

As a next step, the impact of the requirements on the existing PROFINET specifications will be discussed with the respective PI working groups. After that, a mapping of the requirements listed in this document to the IEC 62443-3-3 [7] and 62442-4-2 [25] foundational requirements will be done. This measure shall verify the described concept against the requirements of the two standards referenced.

ACKNOWLEDGMENT

This paper reflects the work of the working group CB/WG10 of PROFIBUS and PROFINET International (PI). The author would like to express his gratitude for the support of the WG and the detailed technical input provided by the WG.

REFERENCES

[1] Statista GmbH, Market share of industrial networks worldwide year 2018, https://de.statista.com/statistik/daten/studie/457627/umfrage/marktanteile-industrieller-netzwerke-weltweit/.

[2] G. Zimmermann, IEEE P802.3cg 10 Mb/s Single Pair Ethernet Task Force Closing Report, http://grouper.ieee.org/groups/802/3/minutes/nov18/1118_cg_close_report.pdf.

[3] J. Hähniche, D. D. Brandt, and D. Xu, "IEEE 802.3cg (10SPE) – 10 Mb/s Single Pair Ethernet meeting Industrial Automation objectives," in ODVA 2017 Industry Conference & 18th Annual Meeting, Palm Habour, Florida, 2017.

[4] National Cybersecurity and Communications Integration Center, Combating the Insider Threat, https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf.

[5] Federal office for information security, Industrial Control System Security: Insiders. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_061.html.

[6] 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.

[7] IEC 62443-3-3:2013 Industrial communication networks - Network and system security-Part 3-3: System security requirements and security levels (+Cor.:2014)

[8] PROFIBUS Nutzerorganisation e.V., PROFINET Security Guideline7.002, https://www.profibus.com/index.php?eID=dumpFile&t=f&f=47893&token=f543743e30d8aa3b51b883d00cdc304926678fe8.

[9] PROFIBUS Nutzerorgansiation e. V., PROFIBUS Security Level 1: Technical Specification for PROFINET, https://www.profibus.com/download/profinet-security-level-1-netload/.

[10] J. Akerberg and M. Bjorkman, "Exploring Security in PROFINET IO," in 33rd Annual IEEE International Computer Software and Applications Conference, 2009: COMPSAC '09 ; 20 - 24 July 2009, Seattle, Washington, USA ; proceedings, Seattle, Washington, USA, 2009, pp. 406–412.

[11] S. Pfrang and D. Meier, "On the Detection of Replay Attacks in Industrial Automation Networks Operated with Profinet IO," in Proceedings of the 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal, 2017, pp. 683–693.

[12] S. Pfrang and D. Meier, "Detecting and preventing replay attacks in industrial automation networks operated with profinet IO," J Comput Virol Hack Tech, vol. 14, no. 4, pp. 253–268, 2018.

[13] Z. Feng et al., "Snort improvement on Profinet RT for Industrial Control System Intrusion Detection," in 2016 2nd IEEE International Conference on Computer and Communications (ICCC): Proceedings: 14 Oct. - 17 Oct. 2016, Chengdu, China, Chengdu, China, 2016, pp. 942–946.

[14] Automation Security 2020 – Design, Implementation and Operation of Industrial Automation Systems, NE 153, 2015. https://www.zvei.org/fileadmin/user_upload/Verband/Fachverbaende/Automation/Messtechnik___Prozessautomatisierung/Namur-Empfehlung_NE_153/PDF/NE153_2015-06-11_de_en.pdf

[15] J. Akerberg and M. Bjorkman, "Introducing security modules in PROFINET IO," in 2009 IEEE Conference on Emerging Technologies & Factory Automation: ETFA 2009 ; Palma de Mallorca, Spain, 22 - 25 September 2009, Mallorca, 2009, pp. 1–8.

[16] M. Runde et al., SEC_PRO - Sichere Produktion mit verteilten Automatisierungssystemen: Schlussbericht für das FHprofUnt-Forschungsprojekt mit dem FKZ 1760A10 sowie 17060B10, urn:nbn:de:bsz:960-opus4-4995. https://serwiss.bib.hs-hannover.de/frontdoor/index/index/docId/499

[17] B. Czybik, S. Hausmann, S. Heiss, and J. Jasperneite, "Performance evaluation of MAC algorithms for real-time Ethernet communication systems," in 2013 IEEE 11th International Conference on Industrial Informatics (INDIN), Bochum, Germany, 2013, pp. 676–681.

[18] T. Muller and H. Dermot Doran, "Protecting PROFINET cyclic real-time traffic: A performance evaluation and verification platform," in 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, Italy, 2018, pp. 1–4.

[19] T. Muller and H. D. Doran, "PROFINET Real-Time Protection Layer: Performance Analysis of Cryptographic and Protocol Processing Overhead," in 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Torino, Italy, 2018, pp. 258–265.

[20] ODVA Inc.: Optimization of Industrial Cyber Security. https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00278R2_Optimization-of-Industrial-Cybersecurity.pdf.

[21] ISO 16484-5: Building automation and control systems (BACS) - Part 5: Data communication protocol, 2017.

[22] A. Shostack, Threat modeling: Designing for security. Indianapolis, IN, Wiley, 2014.

[23] 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.

[24] IEC 62443-2-2:2018 Security for industrial automation and control systems – Part 2-2: IACS protection levels, TC65/717/NP, 2018.

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

[26] W. Speth, "Nur Befehle befolgt: CPS erfordern sichere Identitäten," atp-edition, no. 12, pp. 46–52, 2013.

[27] Runde, Markus, Niemann, Karl-Heinz., Tebbe, Christopher, "Hardware-basierte Informationssicherheit: Einsatz von Security-Token-Technologien," in atp kompakt, vol. 5, Industrielle Informationssicherheit: IT in der Automation, L. Urbas, Ed., München: DIV Dt. Industrieverl, 2014, pp. 16–23.

[28] M. Runde, "Echtzeitfähige Protokollerweiterung zum Schutz Ethernet-basierter Automatisierungskomponenten: Dissertation zur Erlangung des akademischen Grades Doktoringenieur (Dr.-Ing.)," Dissertation, Otto von Guericke Universität, Magdeburg, 2014.

[29] 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/. Accessed on: Jul. 15 2014.

[30] NIST Computer Security Division (CSD), FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC),

[31] PROFIBUS Nutzerorganisation e.V., Security Extensions for PROFINET - PI White Paper for PROFINET, https://de.profibus.com/downloads/pi-white-paper-security-extensions-for-profinet/.