atp magazin

SONDERDRUCK

Transforming Automation
Ausgabe 05 2022

Peer-Review: 02.12.2021

OT security requirements for Ethernet-APL field devices

Technological change can yield improved protection

Karl-Heinz Niemann, Hochschule Hannover, Simon Merklin, Endress + Hauser Digital Solutions

Network convergence is an increasing trend in the automation domain. More and more plant owners strive for a unification of networks in their plants. This yields a seamless network structure, simplified supervision, and reduced training effort for the personnel, as only one unified network technology needs to be handled. Ethernet-APL is one piece of the puzzle for such a converged network, supporting various real time protocols like PROFINET, EtherNet, HART-IP as well as the middleware protocol OPC UA. This paper gives an overview on the impact of Ethernet-APL field devices to OT security and proposes how to ensure OT security for them.

#Ethernet-APL #IT security #field devices

OT-Sicherheitsanforderungen für Ethernet-APL-Feldgeräte

Technologischer Wandel kann verbesserten Schutz bringen

Die Konvergenz von Netzwerken ist ein zunehmender Trend im Bereich der Automatisierung. Immer mehr Anlagenbetreiber streben eine Vereinheitlichung der Netzwerke in ihren Anlagen an. Dies führt zu einer nahtlosen Netzwerkstruktur, einer vereinfachten Überwachung und einem geringeren Schulungsaufwand für das Personal, da nur eine einheitliche Netzwerktechnologie gehandhabt werden muss. Ethernet-APL ist ein Teil des Puzzles für ein solches konvergentes Netzwerk und unterstützt verschiedene Echtzeitprotokolle wie PROFINET, EtherNet, HART-IP sowie das Middleware-Protokoll OPC UA. Dieses Papier gibt einen Überblick über die Auswirkungen von Ethernet-APL-Feldgeräten auf die OT-Sicherheit und schlägt vor, wie die OT-Sicherheit für diese Geräte gewährleistet werden kann.

#Ethernet-APL #IT-Security #Feldgeräte

1. The evolution of system structures in the process industry

The process industry has for many years used system architectures with fieldbus technology in combination with Ethernet on the upper layers. Figure 1 shows the system architecture of an automation system in the process industry.

The sensors and actuators are connected to a remote I/O system via a 4 … 20 mA current loop, usually with additional HART functionality. The remote I/O and other I/O devices, like frequency converters, are connected to the controller via a fieldbus, like PROFIBUS DP. In some plants, a gateway, e.g. a DP/PA coupler, connects the Fieldbus to a Sensor-/Actuator Bus, such as PROFIBUS PA / Foundation Fieldbus H1. The controller is connected to the operator consoles. In many cases the system bus is Ethernet-based and runs either a standardized protocol like PROFINET, Ethernet/IP or a control system specific protocol. Additional servers are often placed between the controllers and the operator consoles. In order to simplify the description, these servers are not shown in Figure 1.

A security appliance connects the control system components on the system bus with the supervisory level represented by the company network. In many cases an additional server is used, e.g. an OPC UA Server. The security appliance (e.g. a multi-port firewall) can be used in such a way, that the server resides in a so-called demilitarized zone (DMZ). The system consists of four networks (company network, system bus, fieldbus, sensor / actuator bus), arranged in a hierarchy.

The field devices, described in the previous section, provide the measurement value and allow digital communication, e.g. for configuration or diagnosis purposes. HART and PROFIBUS PA lack communication speed and are therefore less suited for future applications that require higher bandwidths for asset management, energy management, firmware updates, system backups, etc.

To resolve this deficiency, the use of Ethernet for a sensor/actuator connection could be considered. The standard IEEE 802.3cg [1] specifies a two wire Ethernet that provides power and sufficient bandwidth and that is intended for the connection of sensors, actuators and other devices.

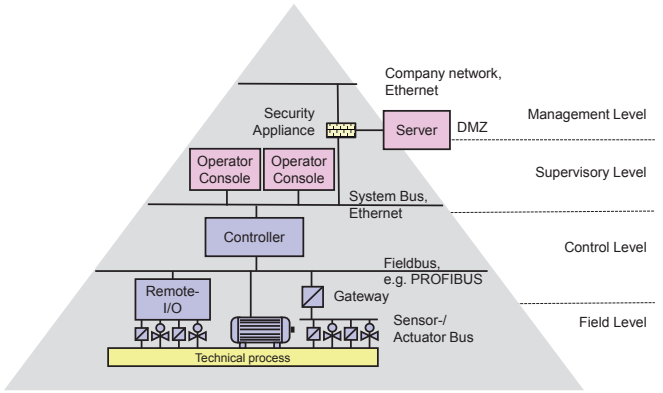

Figure 1: System architecture with Fieldbus, Remote I/O and Sensor-/ Actuator Bus.

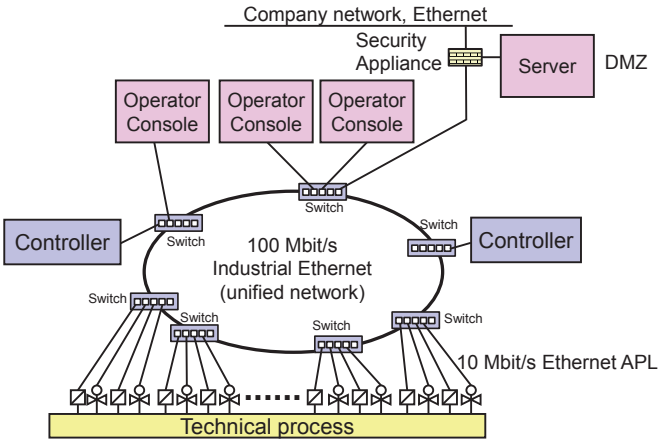

Figure 2: System structure with Ethernet-APL field devices.

Table 1: Comparison of system topologies.

Feature	Hierarchical topology based on different busses with HART	Hierarchical topology based on different busses	Flat topology with Ethernet-APL and Industrial Ethernet protocol.
Variety of communication technologies	Ethernet with Fast Ethernet physical layer, PROFIBUS DP, HART-Protocol	Ethernet with Fast Ethernet physical layer, PROFIBUS DP, PROFIBUS PA	Ethernet-APL and Fast-Ethernet physical layers
Training effort for personnel	Knowledge for all communication technologies listed above needed	Knowledge for all communication technologies listed above needed	Only knowledge for Ethernet needed
Communication of diagnostic data from the device to an asset management system (AMS)	Must pass the different layers of the system. Communication. functionalities in remote I/O and controller needed to pass through the HART diagnostic data to the AMS.	Must pass the different layers of the system. Communication functionalities in controller needed to pass through the PROFIBUS PA diagnostic data to the AMS.	Direct communication between field device and AMS possible. Communication via PROFINET, EtherNet/IP or OPC UA possible.
Communication of measurement values	Via 4 … 20 mA current loop to the Remote IO. Then via PROFIBUS DP to the Controller	Via PROFIBUS PA to the DP/PA Gateway. Then via PROFIBUS DP to the controller	Via Ethernet and protocol like PROFINET or EtherNet/IP to the controller
Accuracy of measurement value transmission	Analog transmission via current loop	Digital transmission	Digital transmission
Available data rate to download a parameter-set to a field device	1,2 kbit/s	31,25 kbit/s	10 000 kbit/s = 10 Mbit/s
Communication mode	Half duplex	Half duplex	Full duplex
Complexity, to access to the device for a cyber attacker	High	Medium	Low

The Ethernet-APL-Group enhanced this standard with a port profile specification [2] that allows the use of the two-wire Ethernet also in rugged environments and in zones with potentially explosive atmosphere at a full duplex communication speed of 10 Mbit/s. The result is called Advanced Physical Layer for Ethernet: Ethernet-APL [3]. Detailed information about the use of Ethernet-APL can be found in [4]. Ethernet-APL is a physical layer for Ethernet that makes it possible to directly connect sensors and actuators to an Ethernet-based network. Possible system structures and the allocation to Ex-zones are shown in [4]. The Ethernet-APL can be combined with a safety profile like PROFIsafe [5]. A short summary is given in [6].

In the context of this paper, it is assumed that the APL field devices are connected to a unified network that combines 100 Mbit/s Industrial Ethernet with Ethernet-APL running with a data rate of 10 Mbit/s as shown in Figure 2.

It can be seen that the layered network approach described in Figure 1 has been replaced by a flat, unified network, as shown in Figure 2. The flat unified network based on Ethernet has several advantages but some disadvantages compared to the hierarchical topology. Table 1 compares the

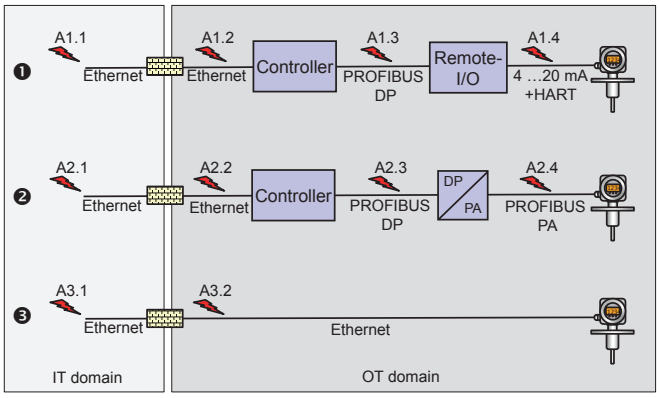

Figure 3: PKI setup in distributed control system.

connection of the field devices with current loop and HART, PROFIBUS PA and Ethernet-APL.
It can be seen that the Ethernet-APL Topology yields a number of advantages: Unified network, high data rates and easy transmission of diagnostic data to an asset management system. But with respect to cyber security, the flat network architecture has a disadvantage: The Ethernet-APL field devices can be attacked more easily by an intruder. The following section will address this issue in detail.

2. The exposition of field devices today and tomorrow

The typical security context of a field device is defined as follows: The plant is protected by a perimeter, like fences or walls. Physical access to the device is only possible for the personnel working in the plant and for external service providers, like commissioning or maintenance personnel. The field device is either connected to the Remote I/O, the Fieldbus (PROFIBUS PA) or the Ethernet network. The Ethernet network is separated from the office network with a security appliance, like a firewall. The field device has no direct connection to the internet.
In general, a field device is exposed to cyber-attacks via various interfaces. This can be a local display in combination with local buttons, Bluetooth, Wireless HART, handheld using wired HART, the current loop, the fieldbus or the Ethernet-APL connection. A detailed risk analysis for a field device that covers all the channels described is available in [7]. This paper will focus on the current loop / HART, the Fieldbus and the Ethernet-APL connection.
The exposition of a field device needs to be set into the context of possible attackers, or attack types and attack locations. For this paper three different locations of attackers will be considered:

» **A1:** Attacker operating in the office network who conquers the security appliance and is able to communicate on the Ethernet network in the OT domain (System bus or unified network according Figure 1 and Figure 2).

» **A2:** Local attacker (inside offender) who has access to the Ethernet network in the OT domain (System bus or unified network according Figure 1 and Figure 2).

» **A3:** Local attacker (inside offender) who has access to the fieldbuses like PROFIBUS DP, PROFIBUS PA or to the current loop with HART and who is able to manipulate the data transmission on these systems.

In addition to the attacker location, two types of attack will be considered. One is a denial of service attack. This prevents authorized access to resources or delays time-critical operations [8]. This attack type leaves the plant inoperable (shutdown) but does not lead to a situation where manipulated IO values might be transferred. This attack type affects the protection goal “availability”. The second attack type involves the manipulation of IO values. This would lead to a situation where the controller reads manipulated, falsified input values, but the attack does not immediately stop the plant, as in the first case. This attack affects the protection goal “integrity”. The following sections will focus on this aspect.
Figure 3 shows 3 different system topologies and possible locations where the field device could be attacked.
Case ❶ describes a Control System with PROFIBUS DP, a Remote IO and a field device that is connected via 4 … 20 mA current loop with HART-protocol. The attackers A1.1, A2.1 and A3.1 reside in the IT domain. Attacking the field device involves the following steps: The attackers A1.1, A2.1 or A3.1 must overcome or bypass the firewall. Then the controller must be manipulated so that commands are issued to the remote IO via PROFIBUS DP that generate false HART commands in the Remote IO, e.g. to change the measurement range of the field device. The attackers A1.2, A2.2 and A3.2 do not need to overcome the security appliance, the rest of the attack is as previously described. It can be seen that the described attack targets the controller in order to manipulate the field device, but it is not possible to directly attack the device itself, as controller and Remote IO are between the attacker and the device attacked.
The attackers A1.3 and A2.3 could attack the PROFIBUS and, for example, insert falsified commands to the Remote IO that issue false HART commands to the field device. In [9] the author describes multiple attack vectors for PROFIBUS DP that apply to PROFIBUS PA as well. Attacker A1.4 could hook up to the current loop and insert false HART commands to the device or even put a resistor in parallel to the device in order to falsify the measurement value. Further attack vectors for HART are described in [10].
Case ❷ describes a Control System with PROFIBUS DP and PROFIBUS PA or Foundation Fieldbus H1. The attack vectors for the attackers A2.1, A2.2 and A2.3 are close to case ❶. Instead of falsified HART commands, falsified PROFIBUS PA commands need to be used, e.g. for device configuration. The attacker A2.4 can hook up to the PROFIBUS PA and directly block or falsify the PROFIBUS PA communication.
Case ❸ represents an automation system that connects the field devices via Ethernet, as Ethernet-APL does. Network switches like Ethernet-APL power switches and APL field switches are transparent to the communication and are not shown in Figure 3. This topology is the easiest one, from the attackers’ point of view. After getting access to the network, the field device can be directly identified and attacked, as it

is part of the PROFINET HART-IP or EtherNet/IP communication. Sample attacks to a PROFINET device are for example described in [11] and [12].
At first glance, case ❸ appears to be the most problematic if no protective measures are applied, as the attackers A3.1 and A3.2 get direct access to the device, without any other devices in between and without any change in transmission media and transmission protocol. However, if the communication to the field device is protected by cryptographic means, the attack is considered more complex compared to case ❶ and ❷. Today, the Standards Developing Organizations (SDOs) already provide or are working on a secure communication for PROFINET [13, 14], EtherNet/IP [15, 16] or OPC UA [17, 18].
The conclusion of this section can be summarized as follows:

- PROFIBUS DP, PROFIBUS PA and HART can be attacked without major effort. Possible attacks are known and documented.
- It is unlikely that HART, PROFIBUS DP or PROFIBUS PA will be upgraded with security functions in the future.
- The only way for secure communication of IO values from the field to the controller is the use of an Ethernet-based protocol in combination with the protocols that support security mechanisms for the protocols used to connect the field devices to the systems.

The outcome is that Ethernet-APL field devices need to support the security functions of the relevant communication protocol (e.g. PROFINET, EtherNet/IP and/or OPC UA). Precautions needs to be considered with respect to computing power, memory size and if necessary, provision of a secure element (e.g. a Trusted Platform Module or similar) . Denial of service attacks must be taken into account to a certain extent, even though the assumption is that the devices are not directly connected to the internet and operate in a protected environment.
The next section will show in detail the security requirements for an Ethernet-APL field device.

3. OT security requirements for Ethernet-APL field devices

For the security requirements definition of Ethernet-APL field devices, the design and protection mechanisms of a process plant with Ethernet-APL fundamental concepts according to IEC 62443-1-1 [19] should be considered.
This step is important, since many component requirements (CRs) and requirement enhancements (REs) of the IEC 62443-4-2 [20] contribute to the fulfilment of the requirements from

Table 2: Security concepts and recommendations and references to further information.

No.	Security concepts and recommendations	Explanation
1	Information Security Management System (ISMS)	An ISMS is the elementary component of a successful implementation of cyber security measures in a process plant and the organization itself. Ideally, the ISMS should be implemented in accordance with IEC 62443-2-1 [21]. Alternatively, it can also be set up according to ISO 27001 [22]. A comparison of the two approaches can be found in [23].
2	Defense in Depth	In principle, it is not recommended to meet the security target with just one protective measure. For this reason, the Defense in Depth approach describes the preference for coordinated protective measures through different security layers in a plant [24]. For further information refer also to [25].
3	Zoning of the plant	It is recommended to divide the process plant into zones with different security target levels. This ensures that each zone of the plant receives the optimum level of security measures [21].
4	Vertical and horizontal segmentation	Zones should be segmented vertically and horizontally. Thus, on the one hand, an attack from the outside is made more difficult (vertical zoning) and at the same time an attack in the case of a compromise on other plant parts can be prevented (horizontal zoning) [21].
5	Zone boundary protection	The zone boundaries of a plant should be protected by appropriate protective measures. This can be done by using security appliances, such as firewalls. When protecting the zone boundaries, the physical access protection of humans should also be considered [21].
6	Protection of communication of field devices and controller	The communication in a zone should be secured by cryptographic methods (integrity and authenticity) [26].
7	Unique proof of identity and authentication of devices in a zone	Devices should be capable to identify themselves in a zone using cryptographic methods [27].
8	Use of secure field devices	The components should be developed according to the Secure Development Lifecycle as per 62443-4-1 [27] and meet the requirements of 62443-4-2 [20].

Table 3: Examples for potential threats and associated protective measures.

No.	Potential threats	Potential protective measures	Reference. to IEC 62443-4-2 [20]
1	Attacker modifies network communication data	Communication integrity and authenticity – Integrity and authenticity of the network communication between Ethernet-APL field devices -should be secured by cryptographic methods. This can be achieved by a secure protocol in combination with a Public Key Infrastructure (PKI) as described in section 4.	CR 3.1/ CR 3.1 RE (1)
2	Attacker participates in network communication without authentication	Authentication of the devices – Ethernet-APL field devices and other components must be able to authenticate each other. This can be achieved by a secure protocol in combination with a Public Key Infrastructure in the plant. (see section 4)	CR 1.8
3	Attacker impersonates APL Field Device	The Ethernet-APL field device must be able to prove the genuity of hardware and firmware. This can be done by means of cryptographic hashes [20].	EDR 3.12
4	Attacker manipulates firmware of the device	The integrity and authenticity of the boot process is a crucial feature to ensure that the device firmware has not been tampered by an attacker. For this reason, the Ethernet-APL field device shall perform authenticity checks during the boot process to ensure that the device does not boot into an insecure or tampered state.	EDR 3.14 EDR 3.14 RE(1)
5	Attacker manipulates firmware through update	The Ethernet-APL field device is able to be updated and only accepts signed firmware from the manufacturer.	EDR 3.10 EDR 3.10 RE (1)
6	Attacker gains access to sensitive data (such as credentials and authenticators) of Ethernet-APL devices	Confidentiality of critical data: The Ethernet-APL field device protects data that is crucial for the secure operation of the plant.	CR 4.1
7	Attacker performs a DoS attack on the network	The APL field device protects itself against DoS attacks in order to maintain the essential functionality of the device. This can be done, for example, by dropping data packets reaching the device that are not relevant for the essential function of the device.	CR 7.1
8	Special requirements for Ethernet-APL field devices, such as long product life and resource constraints	The device design should consider that Ethernet-APL field devices sometimes have very long product lifetimes. An appropriate level of protection of the cryptographic algorithms used should also be considered, as well as the special requirements for resource-constrained devices [26].	---

the concepts mentioned in IEC 62443-1-1 [19]. An excerpt of concepts and recommendations for a secure process plant is shown in Table 2.
An Ethernet-APL field device should be developed according to the Secure Development Lifecycle as per 62443-4-1 [27]. This ensures that R&D implements the security requirements appropriate to the intended use of the device. Examples of successful execution of the process include a Threat Analysis and Requirements Management, a Defense in Depth strategy, Secure Coding Conventions, Security Feature Documentation.
The examples given in Table 3 are a selection of potential threats and protective measures that are necessary for a secure Ethernet-APL field device. Table 3 lists the most important requirements. In order to be able to counter further threats in an Ethernet-APL process plant, additional protective measures are necessary.

4. Secure communication in the OT domain

As described in Section 3, secure communication in the OT environment is one of the central components of a security concept for an Ethernet-APL system. The combination of the use of Industrial Ethernet security concepts, as well as the implementation of a topology analogous to the NOA security concept (Second Channel), promises to solve many OT security challenges [28, 29].
The following section will go into more detail about how to secure the communications of a process plant. The Standards Developing Organizations, such as PI, ODVA and OPC Foundation, use a secured communications protocol in combination with a Public Key Infrastructure (PKI).
This enables:

» Safeguarding of the integrity and authenticity of the communications. It is ensured that the data sent to

a communication peer has not been modified during transmission and was also originated from a trusted communication partner.

» Authentication of devices in the network: The Ethernet-APL field devices in the network communicate only with trusted communication peers.

» Encryption for certain use cases, like configuration data: Some of the communications between components are encrypted. This function makes it impossible for attackers to understand the recorded communication in the network. This supports the confidentiality aspect, e.g. for production recipes.

A Public Key Infrastructure (PKI) is a system that secures the communications of Ethernet-APL field devices and other components by issuing, distributing, validating and possibly revoking digital certificates.
A digital certificate is a digital data record that is structured according to standards such as X.509 [30]. By using digital certificates, it is possible to assign a cryptographic identity to the Ethernet-APL field device, which can be used to identify a device in the PKI system and during connection establishment. Likewise, communications originating from the device can be authenticated by other PKI participants.
A certificate authority (CA) provides a root certificate and signs the sub-CAs signature requests, so that hierarchical trust can be established. The sub-CAs take over the management of the certificates in the various plant sections. Depending on the size of the plant, it may also make sense to introduce sub-CAs in process plants in order to simplify the management of the private keys of the sub-CAs. If a certificate is compromised prior to the end of its lifetime, it can be revoked by means of a Certificate Revocation List (CRL) in the PKI system [31].
Figure 4 shows a possible PKI setup for a company with a distributed plant setting. The Root Certification Authority (Root CA) provides the root of trust for the certificates of the company. Plant sites can then setup their sub-CA in order to provide certificates for that site. All components of the system then receive certificates from that sub-CA as a root of trust for the establishment of a secure communication. A proposal and detailed description of a PKI for use in the decentralized automation systems can be found in [32].
Once the PKI has been set up as shown in Figure 4 and the digital certificates have been distributed to the Ethernet-APL field devices and all other components, they can authenticate each other.
The mutual authentication mechanism takes place during the startup of the communication by sending the respective public key (part of the certificate) to the communication partner, as shown in Figure 5.
The communication partner can use the public key to verify the signed or encrypted data sent by the communication partner. Based on the secure communications established using the asymmetric keys, the devices can then switch to a communication based on symmetric keys, which require

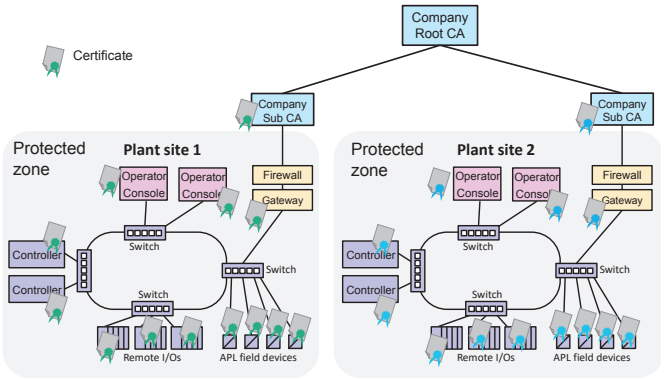

Figure 4: PKI setup in Distributed Control System

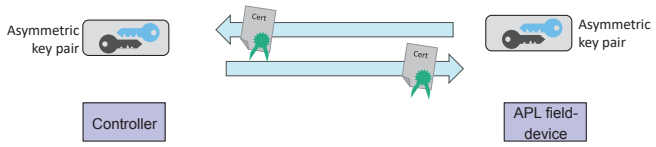

Figure 5: Public key exchange.

less computation effort. For PROFINET, an overview of the secure communication is described in [33]. The corresponding updated PROFINET specifications [34, 35] are currently under review. For EtherNet/IP [36] [16] and OPC UA [17], specifications concerning secure communications are already available.
In order to integrate APL field devices into the communications in a secure manner, they need to support a secured communication protocol, such as PROFINET, EtherNet/IP or OPC UA. All three protocols support or will support a secure communication, as previously described.

5. Summary and outlook

The paper showed that Ethernet-APL Field devices are subject to potential attacks. The flat network structure offers attackers relatively easy access to the devices, as they are directly connected to the plant network. Therefore secure communications will be needed for Ethernet-APL devices. The security requirements for automation components, as described in the IEC 62443-4-2 [20] also apply for APL devices. They need to be treated in the same manner as Controllers or Remote I/Os. By using a secure communication protocol, as outlined in [33], it is possible for the first time to protect the integrity and authenticity of sensor values from the sensor to the controller, which is currently not possible with HART or PROFIBUS PA. In addition to the secure communications, a defense in depth concept should be used to protect the plant area against attacks from the outside. Manufacturers of Ethernet-APL field devices should plan the future integration of a security layer and should reserve sufficient resources in their devices (memory, computing power, possibly a secure element like a Trusted Platform Module or similar).

Referenzen

[1] [Institute of Electrical and Electronics Engineers (IEEE). (2019). *Standard for Ethernet - Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors, IEEE 802.3cg-2019.* Retrieved from: https://standards.ieee.org/standard/802_3cg-2019.html

[2] PROFIBUS Nutzerorganisation e.V. (2021). *Ethernet APL Port Profile Specification: Ethernet-APL Network and Port Requirements.* Retrieved from: https://www.profibus.com/download/port-profile-specification-ethernet-apl.

[3] PROFIBUS und PROFINET Intenational, ODVA Inc., OPC-Foundation, and FieldComm Group. (2020). *Ethernet to the field: White Paper*. Retrieved from: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=107608&token=97abc376e3e83e010df1902d93deba94d1a30d22

[4] Niemann, K. H. (2021). *Ethernet APL Engineering Guideline: Planning, installation and commissioning of Ethernet-APL networks*. Retrieved from: https://www.profibus.com/download/engineering-guideline-ethernet-apl.

[5] Profibus Nutzerorganisation e. V. (2020). *PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO: Profile part, related to IEC 61784-3-3*. Retrieved from: https://www.profibus.com/download/profisafe.

[6] Niemann, K. H. (2021). The Ethernet-APL Engineering Process-A brief look at the Ethernet-APL engineering guideline. *atp magazin, 63*(9).

[7] Niemann, K. H., Hoh, M. (2017). Anforderungen an die IT-Sicherheit von Feldgeräten: Schutzlösungen für hoch vernetzte Produktionsanlagen. *atp magazin, 59*(12), 42-53.

[8] Nieles, M., Dempsey, K., Pillitteri, V. (2017). *NIST Special publication 800-12 revision 1 an introduction to information security*. Gaithersburg: National Institute of Standards and Technology.: Retrieved from https://doi.org/10.6028/NIST.SP.800-12r1.

[9] Igure, V. M. (2012). *Security assessment of SCADA protocols: a taxonomy based methodology for the identification of security vulnerabilities in SCADA protocols*. AV Akademikerverlag.

[10] Bhurke, A. U., Kazi, F. (2021). Methods of Formal Analysis for ICS Protocols and HART-IP CPN modelling. In *2021 Asian Conference on Innovation in Technology (ASIANCON)* (pp. 1-7). IEEE. DOI: 10.1109/ASIANCON51346.2021.9544603

[11] Runde, M. (2014*). Echtzeitfähige Protokollerweiterung zum Schutz Ethernet-basierter Automatisierungskomponenten*. Dissertation, Otto von Guericke Universität, Magdeburg, 2014. URN: urn://nbn:de:gbv:ma9:1-5041. Retrieved from: https://d-nb.info/1057913936/34.

[12] Mehner, S., König, H. (2019). No need to marry to change your name! Attacking profinet io automation networks using DCP. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 396-414). Springer, Cham.

[13] PROFIBUS Nutzerorganisation e.V. (2013). *PROFINET Security Guideline*. Retrieved from: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=47893&token=f543743e30d8aa3b51b883d00cdc304926678fe8

[14] Niemann, K. H. (2019). IT security extensions for PROFINET. In *2019 IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki, Finland, Jul. 2019 - Jul. 2019*, pp. 407–412.

[15] ODVA Inc. (2011). *Securing Ethernet/IP Networks*. Retrieved from: https://www.odva.org/wp-content/uploads/2020/05/PUB00269R1.1_ODVA-Securing-EtherNetIP-Networks.pdf.

[16] Visoky, J., Wiberg, J. (2020). *CIP Security and IEC 62443-4-2.* Retrieved from: https://www.odva.org/wp-content/uploads/2020/05/2020-ODVA-Conference_CIP_Security_and_IEC_62443_Visoky_Wiberg_Final.pdf.

[17] IEC TR 62541-2. (2020). OPC unified architecture - Part 2: Security Model. IEC: www.iec.ch

[18] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2016). *Sicherheitsanalyse OPC UA.* Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/OPCUA/OPCUA.pdf?__blob=publicationFile&v=2.

[19] IEC TS 62443-1-1. (2009). Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models. IEC: www.iec.ch

[20] IEC 62443-4-2. (2019). Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. IEC: www.iec.ch

[21] IEC 62443-2-1. (2010). Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program. IEC: www.iec.ch

[22] EN ISO/IEC 27001. (2017). CEN and CENELEC: Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 with Cor 1:2014 and Cor 2:2015). IEC: www.iec.ch

[23] Niemann, K. H. (2021). *Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443: eine Sicht auf automatisierungstechnische Anlagen der Fertigungs- und Prozessindustrie*. ABB Automation Products GmbH, Heidelberg. Retrieved from https://doi.org/10.25968/opus-1973.

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

[25] Department of Homeland Security. (2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* Retrieved from: https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[26] Niemann, K. H. (2014). IT-Security-Konzepte für die Prozessindustrie. *atp magazin, 56*(07-08), 62-69.

[27] IEC 62443-4-1. (2018). Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. IEC: www.iec.ch

[28] NE 175, NAMUR. (2020). NAMUR Open Architecture - NOA Konzept. NAMUR: www.namur.net

[29] Tauchnitz, T., Ed. (2021*). NAMUR Open Architecture (NOA): Das Konzept zur Öffnung der Prozessautomatisierung, 1st ed.* Essen: Vulkan Verlag.

[30] ISO/IEC 9594-8. (2020). Information technology – Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks. ISO: www.iso.org

[31] Network Working Group IETF. (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280.* Retrieved from: https://datatracker.ietf.org/doc/html/rfc5280.

[32] Tebbje, S., Karthikeyan, G., Friesen, M., Steinke, K., Heiss, S., Niemann, K. H. (2020). *Entwicklung einer IT-Sicherheitsinfrastruktur für verteilte Automatisierungssysteme: Schlussbericht zu IGF-Vorhaben Nr. 19117 N*. https://doi.org/10.25968/opus-1626.

[33] PROFIBUS Nutzerorganisation e.V. (2019). *Security Extensions for PROFINET - PI White Paper for PROFINET*. Retrieved from: https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/.

[34] PROFIBUS Nutzerorganisation e.V. (2021). *Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO: Version 2.4 MU3.* Retrieved from: https://www.profibus.com/download/profinet-specification.

[35] PROFIBUS Nutzerorganisation e.V. (2021). *Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO: Version 2.4 MU3.* Retrieved from: https://www.profibus.com/download/profinet-specification.

[36] ODVA Inc. (2020). *Overview of CIP Security*. Retrieved from: https://www.odva.org/wp-content/uploads/2020/05/PUB00319R1_CIP-Security-At-a-Glance.pdf.

AUTOREN

Prof. Dr.-Ing. Karl-Heinz Niemann (born 1959) represents the areas of industrial informatics and automation technology at Hannover University of Applied Sciences and Arts since 2005. From 2002 to 2005, he was responsible for the area of process data processing at the University of Applied Sciences and Arts Northeast Lower Saxony (today Leuphana University). Prior to that, he held leading positions in the development of process control systems, at ABB, Elsag Bailey and Hartmann & Braun.

Prof. Dr.-Ing. Karl-Heinz Niemann
Hochschule Hannover
Fakultät I – Elektro- und Informationstechnik
Postfach 92 02 61
30441 Hannover
✆ +49 511 92 96 12 64
@ karl-heinz.niemann@HS-Hannover.de

M. Sc. Simon Merklin (born 1989) is Cyber Security Specialist and leader of the Product Security Marketing working group at Endress+Hauser. He graduated at the Karlsruhe Institute of Technology in Business Informatics with focus on security and cryptography and wrote his master's thesis about Distributed Ledger Technologies. Furthermore, he participated in the IEC 62443-4-1 certification of Endress+Hauser and is member of the PROFINET Security Working Group at PROFIBUS and PROFINET International.

M. Sc. Simon Merklin
Endress+Hauser Digital Solutions
Christoph Merian-Ring 12
4153 Reinach
Switzerland
@ simon.merklin@endress.com