Joint Working Group

FieldComm Group, ODVA, OPC Foundation, PROFIBUS & PROFINET International

SECURE DEPLOYMENT OF INDUSTRIAL COMMUNICATION PROTOCOLS: A RISK MANAGEMENT BASED APPROACH

Disclaimer

Prepared by Joint Working Group Device Tool Security for Ethernet and non-Ethernet-based Communication, consisting of the Standards Developing Organizations (SDOs) (alphabetical order):

- FieldComm Group
- ODVA, Inc.
- OPC Foundation
- PI (PROFIBUS & PROFINET International)

Contributing core group members (alphabetic order):

Adam Schneider (Emerson), Alexander Meurer (BASF), Andreas Gutscher (Balluff), Anis Ahmad (Emerson), Arne Felber (CodeWrights), Benjamin Reibold (Pepperl+Fuchs), Bhavik Zala (Emerson), Christoph Spiegel (Krohne), Christopher Saile (Pepperl+Fuchs), Dilara Madinger (Emerson), Dmitry Gringauz (Banner Engineering), Dorenburg (Knick), Dominic Dekerf (Cargill), Edwin van Hoeven (Yokogawa), Felix Reichert (SEW-Eurodrive), Florian Allgaier (Vega), Florian Sieber (Festo), Francesco Rovelli (Endress+Hauser), Frank Fengler (ABB), Gunnar Lessmann (Phoenix Contact), Harald Müller (Endress+Hauser), Jack Visoky (Rockwell Automation), Joakim Wiberg (ODVA), Josh Harmon (Delta Motion), Kai Hackenstrass (ifm), Kurt Polzer (Polzer Automation Solutions), Matthias Reiter (Festo), Matthias Schmidt (ifm), Mathias Monse (Sipos), Mirko Brcic (Endress+Hauser), Noah Paulat (Vega), Olliver Lundmattsson (Emerson), Pascal Sarrazin (Markem-Imaje), Philipp Ketterer (Vega), Randy Armstrong (OPC Foundation), Rob Umfreville (Rotork), Roberth Asplund (Emerson), Sebastian Broschei (Softing), Sebastian Heidepriem (SICK), Sean J. Vincent (FieldComm Group), Stefan Schaefermeyer (ifm), Stephen Mitschke (FieldComm Group), Sven Giesecke (CodeWrights), Ulrich Raithel (Sipos), Varsha Shinde (Emerson), Werner Laengin (AUMA), W. Kuipers (Krohne), Yasuki Yoda (Omron), Dominik Ziegler (Siemens)

Comments to be submitted to Working Group editor: simon.merklin@endress.com

This technical paper exclusively describes the capabilities of industrial communication protocols and does not guarantee compliance with legal requirements, like the Cyber Resilience Act.

Table of Contents

Intended audience

System integrators, product suppliers and assessors interested in learning how to deploy industrial communication protocols in a secure way using a risk-based approach.

Assessors to provide base protocol security capabilities, general risk assessment and possible counter measures.

End users of industrial communication protocols, such as plant operators, who want to deepen their understanding of how to use these protocols securely.

Executive summary

Industrial communication protocols are a foundational element of modern process and factory automation, enabling interoperability, real-time control, and efficient device integration. However, many widely deployed protocols were not originally designed with cybersecurity as a primary objective. Although standards development organizations have been steadily adding security functionality to these protocols, there are still many deployments that lack built-in security mechanisms such as authentication, authorization, integrity, and confidentiality.

To address this challenge, FieldComm Group, ODVA, OPC Foundation, and PROFIBUS & PROFINET International have collaborated to establish a shared operational environment and architecture overview for industrial communication protocols in alignment with EN 40000-1-2 [1]. Based on the EN 40000-1-2, in this technical paper, a structured risk-based methodology is applied to assess cybersecurity risks associated with commonly used industrial communication protocols and to define appropriate mitigation strategies.

The assessment confirms, that in many cases, the use of industrial protocols relies heavily on additional compensating controls provided by the operational environment. Even as Ethernet-based protocols such as EtherNet/IP, HART-IP, OPC UA, and PROFINET offer enhanced security profiles, their usage depends on the risk assessment and operational environment of the end user.

Motivation and scope

The four Standards Development Organizations (SDOs), FieldComm Group, ODVA, OPC Foundation, and PROFIBUS & PROFINET International, have joined forces to strengthen cyber resilience in industrial automation and control systems. Note that for industrial protocols which are not maintained by these four SDOs this technical paper does not make any explicit claim, but the information here is likely generalizable to other industrial communication protocols.

This technical paper aims to provide guidance for industrial communication protocols usage in alignment with the EN 40000-1-2 [1].

By establishing a common understanding of how to securely deploy and use industrial protocols, this document helps:

- Automation product vendors to better understand the security risks associated with implementing and supporting industrial protocols in products.
- Assessors to have a common understanding of communication technology feasibilities.
- System integrators and end-users to implement protocols in a way that ensures operational security and regulatory compliance.

The examples presented here combine protocol-specific security features with additional compensating controls in the operational environment, forming a holistic approach to mitigating cybersecurity risks.

This technical paper also aims to address how these protocols are expected to be used considering the Annex I requirements of the Cyber Resilience Act (CRA) [11]. While there are

many requirements in Annex I of the CRA, the focus for this paper is on requirements related to authentication and protection of data in transit, as industrial protocols are directly implicated in these. Other protocol-dependent requirements such as logging, while relevant, are not addressed in this paper. The CRA applies to products, not the communication protocols themselves. Consequently, many CRA requirements are product-specific and remain mandatory regardless of which communication protocols a product implements. Furthermore, the usage of a communication protocol may vary from product to product which could affect the risk; therefore, the analysis done in this paper is necessarily generic and further analysis is necessary to make any given product CRA-compliant.

Industrial communication protocols in scope of this paper:

- DeviceNet
- EtherNet/IP
- FOUNDATION Fieldbus
- HART 4-20mA
- HART-IP
- IO-Link
- OPC UA
- PROFIBUS PA
- PROFINET
- WirelessHART

Methodology: Risk-based approach

The cybersecurity principles and risk-based approach of the EN 40000-1-2 [1] is followed for the usage of the industrial communication protocols in scope. According to the EN 40000-1-2 the risk-based approach includes:

- Defining the product context
- Risk assessment
- Risk treatment
- Risk communication
- Risk monitoring and review

The following sections document the main results of the risk-based approach to industrial communication protocols. For clarity, the term "product" (as defined in EN 40000) has been replaced with "industrial communication protocol".

International Cybersecurity Standard IEC 62443

IEC 62443 is the international standard series that provides a complete framework for cybersecurity of Industrial Automation and Control Systems (IACS) [11]. IEC 62443 is deliberately risk-based and lifecycle-oriented. It requires a structured risk assessment to determine the appropriate Security Level (SL 1–4) for each zone and conduit, then applies only the controls necessary to achieve that level using the seven Foundational Requirements

(Identification & Authentication Control, Use Control, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events, and Resource Availability).

IEC 62443 is a standard that applies to asset owners or operators and others in the supply chain—it is explicitly designed as an encompassing ecosystem of responsibilities shared across the entire supply chain. Different parts of the standard series are targeted at different roles:

- **IEC 62443-2-x** → Policies, processes, and requirements for asset owners and operators
- **IEC 62443-3-x** → System-level requirements for integrators and solution providers
- **IEC 62443-4-x** → Component-level requirements (including secure development lifecycle) for product suppliers and manufacturers

This deliberate partitioning ensures that every party—owner-operator, service provider, system integrator, and product supplier—has clear, mandatory obligations. Security is treated as a shared responsibility from product design through decommissioning.

Zone and Conduit Model
The cornerstone of IEC 62443 system-level security is the Zones and Conduits model (defined in IEC 62443-3-3 and IEC 62443-1-1). A Zone is a logical or physical grouping of assets that share common security requirements, trust level, and risk exposure. A Conduit is a secure communication path that connects zones (or assets within a zone) while enforcing the required security policies for that connection. The model forces explicit identification of trust boundaries: assets inside the same zone are assumed to trust each other to the degree required by the zone's Security Level, while every conduit must implement controls sufficient to protect against threats crossing that boundary.

Industrial communication protocol context

The primary purpose of industrial communication protocols is connecting field devices with control systems in process and factory automation. While they share the common goal of enabling configuration, diagnostics, and data exchange, they differ from a technological side:

- **Ethernet-based industrial communication protocols** leverage standard Ethernet and TCP/IP for control and motion applications. Industrial protocols in this category are:
    - EtherNet/IP
    - OPC UA
    - PROFINET
    - HART-IP
- **Non-Ethernet based industrial communication protocols** can include point-to-point communication that combines analog 4-20 mA or binary signals with digital signals with digital communication or fieldbuses that use automation control specific transportation and protocol layers for fully digital bus communication. Industrial protocols in this category are:
    - HART
    - IO-Link
    - FOUNDATION Fieldbus
    - PROFIBUS
    - DeviceNet

Note that in many cases there will be second channel protocols that allow operations such as configuration, diagnostics, etc. An example of this is a field device which implements HART but also has a Bluetooth Generic Attribute Profile (GATT) interface for configuration. Second channel protocols carry their own unique risks which need to be assessed and appropriately mitigated, per a risk assessment. However, second channel protocols are not within the scope of this paper. There is also the possibility of running non-Ethernet industrial protocols over a wireless transport, in something like WirelessHART. Although these are non-Ethernet protocols, they have similar risk profiles as Ethernet-based industrial protocols and therefore will need similar security protections as the Ethernet-based industrial protocols.

Together, these protocols form the backbone of modern industrial automation, ensuring interoperability, real-time data exchange, and efficient device integration across diverse environments.

Intended purpose and functions

These industrial communication protocols are deployed in a wide variety of environments and applications. They are commonly used in industries such as, but not limited to, these:

- Water/wastewater
- Food/beverage
- Power/energy
- Life sciences
- Chemical
- Oil/gas
- Primaries/metals
- Packaging
- Tooling machines
- Robots
- Automotive manufacturing

Although these industrial communication protocols are deployed in a broad spectrum of industries, environments, and applications they serve comparable use cases, including:

- Control of motion of physical systems such as motors and robotic arms
- Transmission of safety relevant data
- Configuration of industrial equipment for a particular machine or application
- Exposure of diagnostic information
- Cyclic real time data exchange that reflects (input) or impart (output) some physical characteristic on a system like temperature, pressure, etc.

Misuses to Avoid

The following actions are considered misuses and may lead to hazards:

- Operating the product for purposes other than those intended.
- Ignoring safety warnings or removing protective components.
- Using the product in extreme conditions beyond those specified.
- Installing the product in operational environment that aren't protected by physical access controls.

Industrial communication protocols are deployed in a wide variety of systems and industries. Those communication protocols are typically used at levels 0–2 of the Purdue Model [16], where there is strict segmentation of various levels, and occasionally at higher levels. Their use spans communication within a machine, between machines, and throughout process industry plants. Typical use cases are controlling physical motion or processes in plants, e.g., a motor controlling a press. An interconnected system could have anywhere from two nodes up to hundreds of nodes with routable communication.

Operational environment and architecture overview

This section describes the operational environment of industrial communication protocols and gives examples. This includes the reasonable usage regarding the location of industrial communication protocols in the architectures, such as the Purdue Model and an Industrial Internet of Things (IIoT) model, and assumptions regarding available protection mechanisms within the plant installation (e.g., firewalls or physical access restrictions).

Location in the network

Industrial protocols can exist in many locations within an industrial network. One widely used method is to follow the Purdue Model. This is discussed in various documents such as IEC 62443-1-1 [12], the NAMUR NA 169 [13], and the hierarchical classification of an IACS in accordance with 62443-1-1 [12]. In most cases, industrial protocols, especially the non-Ethernet ones, are used in layers one and two within the Purdue Model. However, Ethernet-based industrial protocols are often used at higher levels, in some cases even including cloud connectivity.

Besides the Purdue Model, some industrial environments are organized in more of an IIoT scheme (for example, the Industrial Internet Consortium Reference Architecture [17]) where industrial devices have higher level connectivity, especially through the use of Ethernet-based industrial protocols. In this scheme, Ethernet routing is used to allow connectivity to PLCs, field devices, and other industrial nodes.

Most large installations do not strictly adhere to strict layers; typical use is to have isolation and segmentation applied to some parts of the network and connectivity applied to others. As such these models shouldn’t be seen as strict categories but rather methodologies that can be mixed and applied as necessary for the end user, of course with an analysis of the risk trade-offs for usage of any model.

To that end, several examples are presented in this paper. Examples may be combined, and the details can vary significantly with regard to the technologies used. The examples are high-level and focus on showing a specific technical control for mitigating industrial protocol risk, therefore there are necessary technical details about the deployment or environment left out of the examples. However, it is the hope that these examples provide some information on reasonable use of industrial protocols and the security properties thereof.

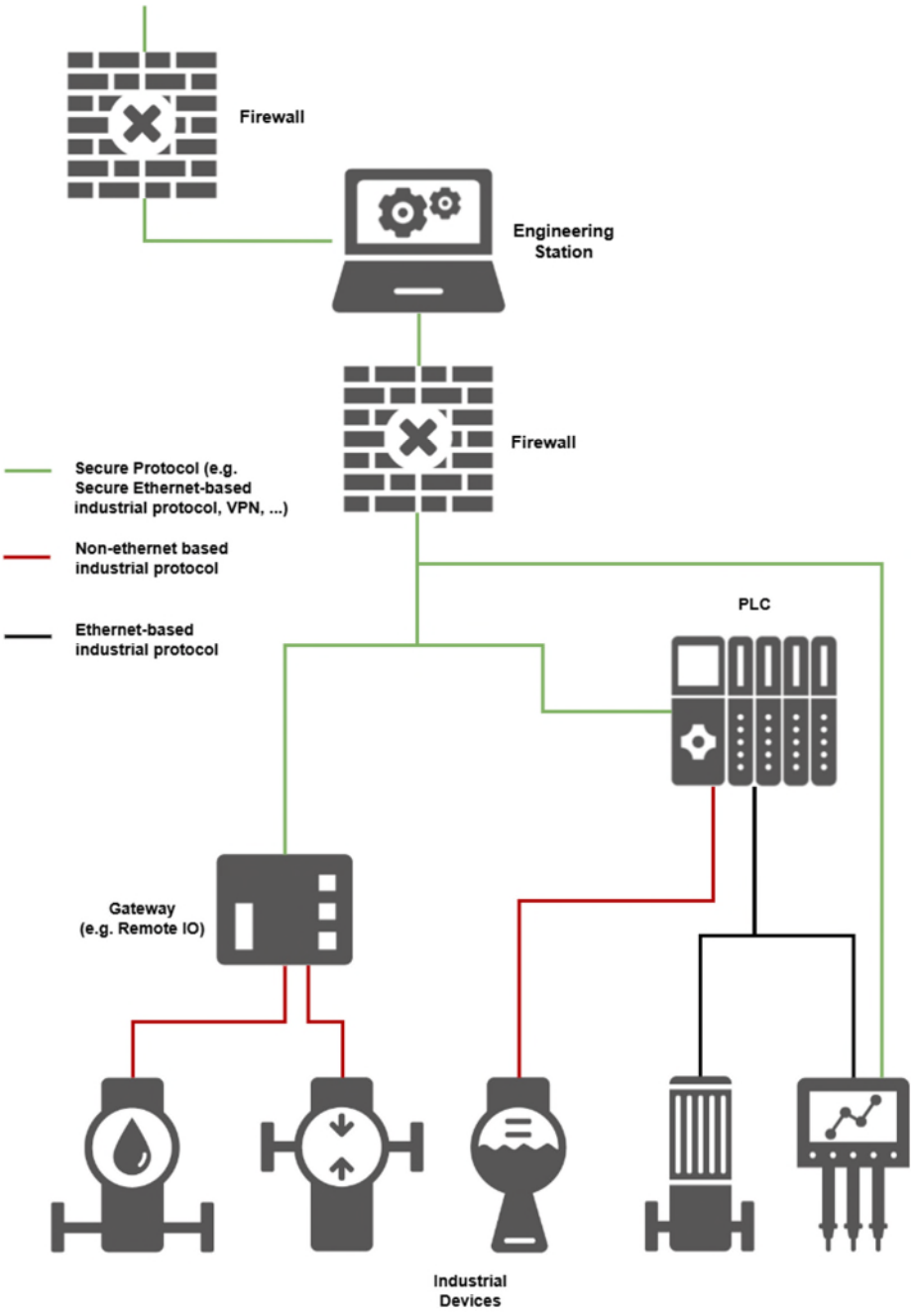

Figure 1. Typical industrial communication protocol architecture according to Purdue Model

For more detailed industrial communication protocol architectures, please refer to the secure deployment guidelines of the respective industrial communication protocol.

Deployment recommendations and examples

Applications where industrial protocols are used can vary widely. However, each usage needs to consider the risk related to the communication and apply appropriate additional compensating controls, specifically considering authentication and protection of data in transit. The Ethernet-based industrial protocols provide advanced security features directly within the protocol that can mitigate these risks directly and are recommended to be used when available. However, environmental compensating controls can also be used to protect the data transmitted by these protocols, as shown in the examples. Non-Ethernet-based industrial protocols have different risk factors due to their nature, and it is recommended that these protocols are isolated to as small a network as feasible. If data is needed from these protocols in other networks, additional compensating controls like secure gateways need to be applied to ensure protection

of that data. In the future the SDOs will provide more detailed secure deployment guidelines for their industrial communication protocols.

Although each deployment of industrial protocols needs a threat model/risk assessment to be performed, the essential recommendations of this paper can be summarized as follows:

- For Ethernet-based industrial protocols, enable the built-in security features based on the risk assessment
- For non-Ethernet based industrial protocols, ensure that the network is sufficiently isolated to reduce risk to an acceptable level
- For a heterogeneous communication environment, enable built-in security features on any gateway/bridge device that connects Ethernet and non-Ethernet protocols so as to keep the non-Ethernet based industrial protocols sufficiently protected
- For interoperability with legacy Ethernet devices, some of the built-in security features may be disabled, if there are sufficient environmental countermeasures to reduce the risk

Physical security / secure cell concept and examples for deployment are described below.

Physical security / secure zone concept

All deployments of industrial protocols depend on physical security of the plant. It is not feasible for industrial protocols to defend against a direct physical attack, and it is expected even under reasonably foreseeable use that the physical environment is secured against unfettered access by would-be attackers. The exact physical compensating controls will vary depending on the risk assessment, but all deployments need at least some physical barriers against unauthorized access to the industrial protocols to prevent unfettered access. Even with significant security measures applied to the protocols themselves (e.g. CIP Security, HART-IP V2, OPC UA, PROFINET Security, etc.), physical security is still a risk that needs to be mitigated by environmental controls. As such, it is assumed that only individually authenticated and authorized personnel of the operating company can access the operational environment and the third-party personnel can only access the plant with supervision of trained staff. Other environmental controls for physically securing a zone could be, e.g.:

- Conduits:
  Conduits are controlled communication channels that connect different security zones. When implemented as an external counter measure, conduits ensure that data exchange between zones occurs in a secure and monitored manner
- Restricted physical access to communications (e.g. physical access to the wires)
- Components that support industrial communication protocols are physically protected e.g., locking doors/cabinets, surveillance, etc.

Example #1 Complete Isolation (Ethernet and Non-Ethernet Industrial Protocol)

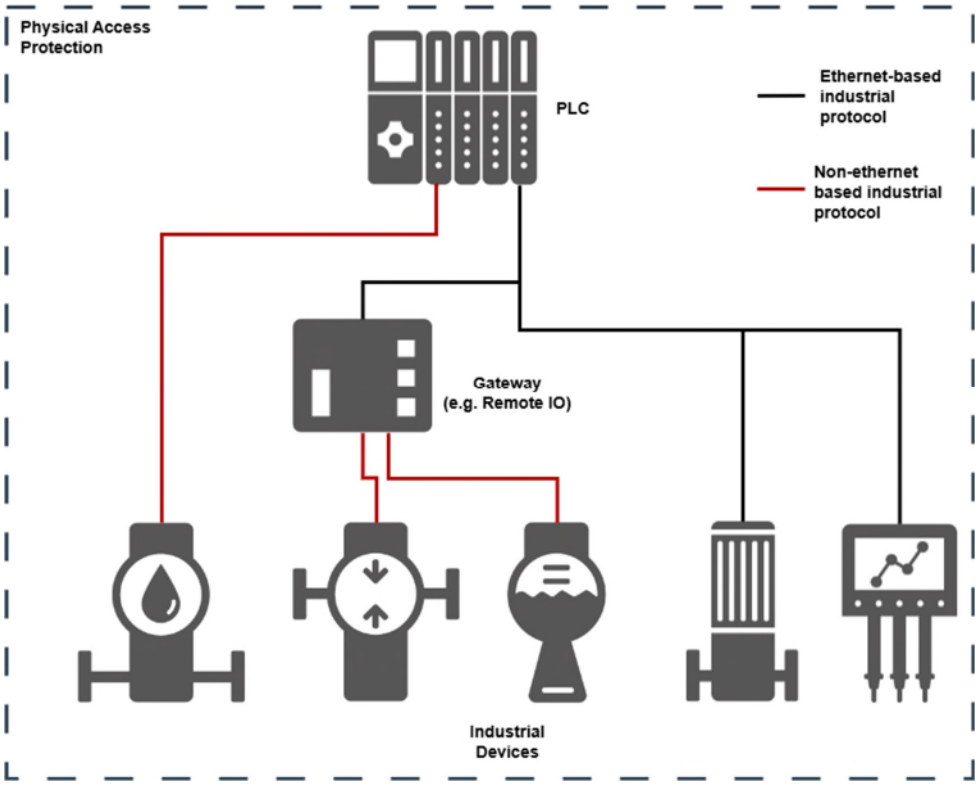

Figure 2. Complete Isolation (Ethernet and Non-Ethernet Industrial Protocol)

The example of the industrial network shown in Figure 2 is completely isolated from any other network. In many cases this provides significant risk reduction, especially if the network is sufficiently small. The example given in the diagram shows several devices connected by a non-Ethernet-based industrial protocol. There is a connection to a gateway device, and through that gateway a connection to a PLC over an Ethernet-based industrial protocol. The network is quite limited (5 devices, a gateway and a PLC) without any connectivity to a larger network. Of course, this is just one possibility to create an isolated industrial network, several variations would exist. However, it is important to keep in mind that a scheme like this depends heavily on the security properties of the environment. That is, physical access must be restricted such that it is sufficiently difficult for an attacker to physically connect to the network as to render these attacks low risk. This can be achieved via protections such as security guards, badge access-controlled rooms, gates, monitoring systems, etc. Furthermore, the larger this network is made both in the sense of number of devices and physical expansion of the network the more difficult it is to control access. Therefore, special care needs to be taken to ensure that the physical protection is applied in an informed, risk-based manner. However, when it is used in this way it does provide significant risk reduction with respect to authentication and data confidentiality and data integrity. That is, if an attacker cannot reach the network or the devices on it then the attacker cannot launch attacks on the data or devices within the network.

Example #2 Gateway Protection (Ethernet and non-Ethernet Industrial Protocol)

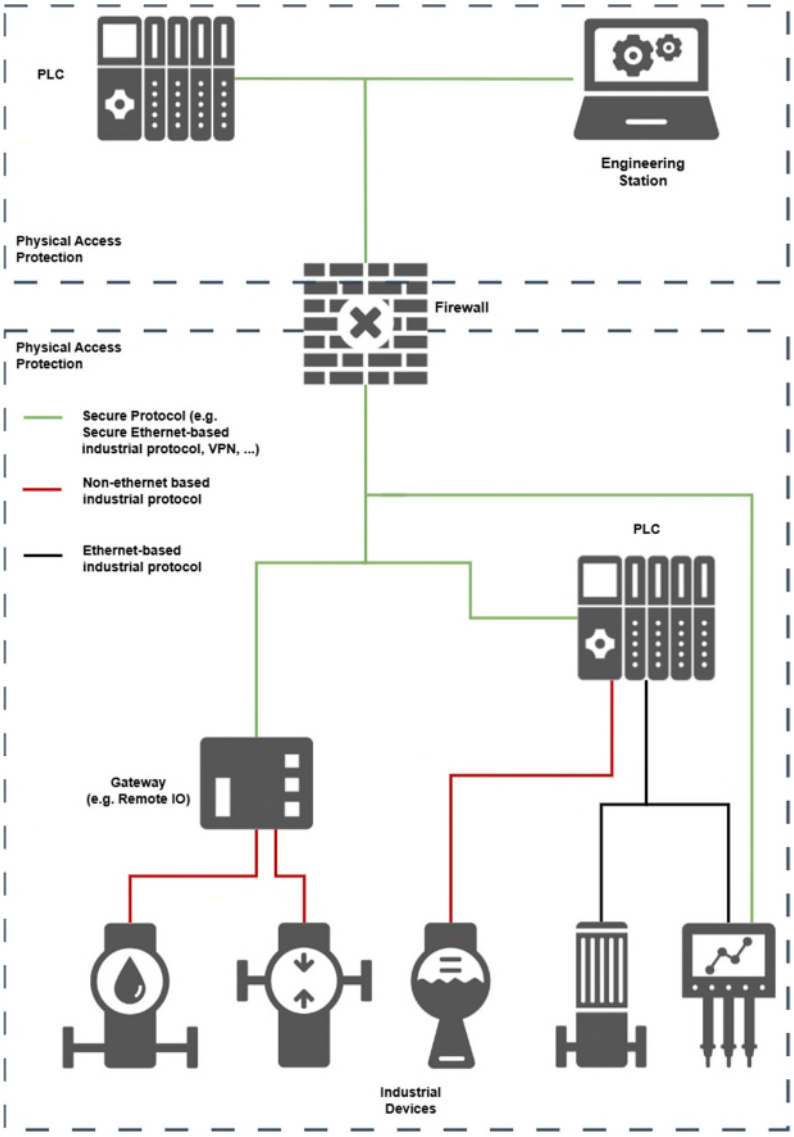

Figure 3 Gateway Protection (Ethernet and non-Ethernet Industrial Protocol)

The example shown in Figure 3 compares to Example #1, but now data from the non-Ethernet industrial protocol network is exposed to a larger network via a secure gateway and routed/switched network. In this case the non-Ethernet industrial protocol network remains isolated as is with Example #1, but here the gateway provides security functionality for accessing to the data on the non-Ethernet network. Note that the gateway can be implemented in a dedicated gateway device, or within a multipurpose device like a PLC; both of these are shown in the example in Example #3 shown in Figure 4. The gateway provides protections via an industrial protocol with security provided by mechanisms like TLS, using certificates as authenticators and applying data confidentiality and data integrity to any data transmitted on the Ethernet network. Again, this is simply an example, many variations of this scheme exist. However, the main idea here is that a gateway exists to provide security functionality on behalf of the non-Ethernet industrial protocol devices, allowing their data to be exposed on a larger network with sufficient protections.

Example #3 Secure Protocol (Ethernet-based Industrial Protocol)

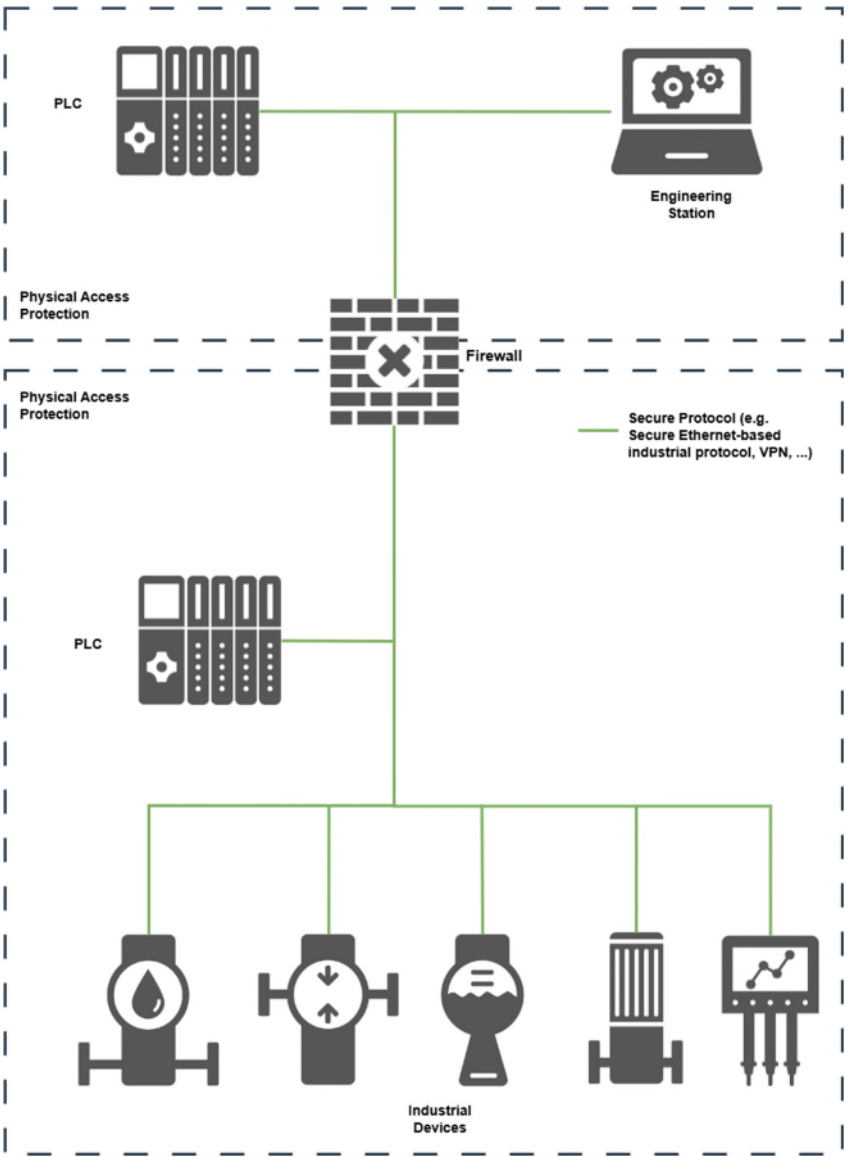

Figure 4. Secure Protocol (Ethernet-based Industrial Protocol)

In the example shown in Figure 4 the devices use an Ethernet-based industrial protocol with the built-in protocol security measures enabled. This might be OPC UA security, EtherNet/IP with CIP Security, PROFINET Security or HART-IP with security. The exact configuration options for any one of these given technologies will vary based on the specific use case, but in this example, they have been enabled to provide authentication for the industrial protocol, as well as protection of the data in transit. This provides very significant risk reduction and can be applied to nearly any network design, as the communication of the industrial devices is protected and can operate in networks with varying levels of trust and additional compensating controls. Zones of trust can be set up however a user wishes, as each device has the capability to enforce trust per the user's design. For Ethernet-routed industrial communication, this use case represents the best case of device defence and can work in a zero-trust enabled environment.

User description

The users/administrators of industrial automation equipment are expected to have a certain profile and attributes. Note that industrial automation equipment is a different category from something like consumer electronics, and therefore the user profile is different. This section gives information about some common attributes of the users/administrators, which is important to keep in mind when evaluating the security of industrial protocols.

User profile

- User Type: Professional personnel for process and/or factory automation
- Environment: Process and/or factory automation
- Tasks: Installation, operation, maintenance, and decommissioning

Competence level

- Expertise: Trained in his/her field of operation, e.g., in process control, safety regulations, and regulatory standards

Regulatory context

- Compliance: Strict adherence to internal guidelines

Expected behavior

- Always acts according to internal guidelines
- Complies with safety and compliance requirements

Based on the user description, it is expected that industrial protocols are deployed securely according to the deployment recommendations of the SDOs.

Conclusions

All of the non-Ethernet-based industrial communication protocols lack basic security capabilities such as authentication, authorization, integrity, or confidentiality protection. Conversely, all of the Ethernet-based industrial communication protocols have security protections defined that include authentication, authorization, integrity, and confidentiality.

Non-Ethernet-based industrial protocols expected use is within an environment that is not routable or reachable by higher layers of the plant and therefore are isolated to a secured network. If data from these protocols is made available to larger networks with different security properties and risks, it should be done through a product with gateway/network translation functionality, at which security controls can be implemented. Furthermore, Clause 55 of the Cyber Resilience Act [11] discusses how certain CRA requirements are not applicable to some products for the purpose of interoperability. These non-Ethernet-based industrial protocols rely on functionality without state-of-the-art security features like authentication or encryption for interoperability purposes. Therefore, the threat risk assessment counter measures for non-Ethernet-based industrial protocols rely heavily on other means than security measures implemented directly in these protocols. Additional compensating controls, like limiting the industrial communication protocol to trusted environments is described within the examples of this document.

Ethernet-based industrial communication protocols have specified security profiles that meet or exceed widely recognized mechanisms for product protection.

Examples are:

- EtherNet/IP with its security functionalities
- HART-IP with its security functionalities

- OPC UA with its security functionalities
- PROFINET with its security functionalities

The security protections of the Ethernet-based industrial protocols allow them to be used in a wide variety of environments with varying levels of risk. That is, they can be used in environments with a significant number of additional compensating controls, or they can be used in environments with few additional compensating controls since they include security protections for the protocols themselves. Of course, it will be a decision of the plant owner/operator based on risk assessment what additional compensating controls to deploy and what protocol security functionality to configure.

The specification, implementation, and market adoption of industrial ethernet security functionalities is a constantly evolving process. Therefore, one solution for end users is, to treat industrial ethernet protocols without security functionalities the same way as non-Ethernet-based industrial protocols.

Summary and outlook

Industrial communication protocols form the backbone of modern automation systems, yet most of them were not originally designed with cybersecurity in mind. While Ethernet-based protocols like EtherNet/IP, HART-IP, OPC UA, and PROFINET offer enhanced security profiles because of the wide variety of use cases they enable, non-Ethernet Industrial communication protocols require compensating measures than the Ethernet-based protocols at the operational environment level.

A holistic approach combining protocol-specific security features with robust physical, technical, and organizational measures in the plant environment is essential. Concepts such as perimeter protection and zero-trust architectures will play a critical role in mitigating risks, especially for protocols without native security capabilities.

Looking ahead, the following developments are expected to shape the secure use of industrial protocols:

- **Alignment with regulatory frameworks:** The Cyber Resilience Act will drive harmonization of security requirements across Europe. Future guidelines will need to integrate CRA principles with IEC 62443 practices.
- **Evolution of protocol standards:** Standards Development Organizations (SDOs) are actively working on extending security functionalities for existing ethernet protocols and defining best practices for deployment.
- **Increased adoption of secure profiles:** Ethernet-based protocols with advanced security features will become more relevant in critical environments, reducing reliance on external additional compensating controls.
- **Operational environment hardening:** Plant operators will increasingly implement layered defence in depth strategies, including network segmentation, strict access control, and continuous monitoring.
- **Collaboration and knowledge sharing:** Continuous cooperation between SDOs, product suppliers, integrators, and end-users will be vital to ensure interoperability and maintain security across heterogeneous systems.

In conclusion, achieving secure industrial communication requires a shared responsibility model between protocol developers and plant operators. Future work will focus on refining security guidelines, developing reference architectures, and supporting industry stakeholders in implementing resilient solutions.

Possible topics for next version of this document

The Joint Working Group will follow up its work on this paper for a next version.

Possible topics to work on are:

- Inclusion of the NAMUR Open Architecture concept
- Mapping of the Industrial Communication Protocols to Annex 1. ESSENTIAL CYBERSECURITY REQUIREMENTS of the Cyber Resilience Act

Definitions, abbreviations, references, version history

Term	Description
Intended purpose	‘Intended purpose’ means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation
Reasonably foreseeable use	‘Reasonably foreseeable use’ means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions
Device	Defined within Class ABA751-Transmitter, ABD340-Final control element , ABN977-Infrastructure device, ABP397-Process analyser (and underlying products with digital elements) as described under IEC - Common Data Dictionary (CDD) Characterization [18].

Abbreviations

Term	Description
IACS	Industrial automation and control system
SDO	Standards Development Organization
PI	PROFIBUS and PROFINET International
OT	Operational Technology
SIS	Safety instrumented system
PLC	Programmable logic controller
DREAD	Damage, Reproducibility, Exploitability, Affected Users, Discoverability
CRA	Cyber Resilience Act
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
IEC	International Electrotechnical Commission

References

[1] EN 40000-1-2:2025-11 – Draft
Cybersecurity requirements for products with digital elements - Part 1-2: Principles for cyber resilience; English version prEN 40000-1-2:2025
Autor: Technical Committee CEN/CLC/JTC 13
Link: https://www.dinmedia.de/en/draft-standard/din-en-40000-1-2/396310071

[2] Cyber security in the oil and gas industry based on IEC 62443
Autor: DNV GL

[3] Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
Autor: BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Link: https://www.bdew.de/media/documents/BDEW-OE-VSE-Whitepaper-3.0.pdf[4]
Secure Architecture for Industrial Control Systems
Autor: SANS Institute
Link: https://sansorg.egnyte.com/dl/6df6HbVkFWcx

[5] IT-Sicherheitsleitfaden; Web-Applikation zum DWA-M 1060
Autor: DWA

[6] Regulatory Guide - CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES
Autor: U.S. Nuclear Regulatory Commission

[7] Practical Security Recommendations for building OPC UA Applications
Author: OPC Foundation

[8] Security Extensions for PROFINET – PI White Paper for PROFINET
Autor: PNO

[9] THE CIP NETWORKS LIBRARY
Autor: ODVA, Inc.

[10] OT-Security für Ethernet-APL – Architektur und Feldgeräte für den sicheren Betrieb
Link: https://www.researchgate.net/publication/394838616_OT-Security_fur_Ethernet-APL_Architektur_und_Feldgerate_fur_den_sicheren_Betrieb
Autor: Meurer, A.; Hout, F.; Merklin, S.; Floeck, M.

[11] Cyber Resilience Act
Autor: European Union
Regulation - 2024/2847 - EN - EUR-Lex

[12] Security for industrial automation and control systems – Part 1-1: Terminology, concepts and models
Author: International Electrotechnical Commission
Link: https://webstore.iec.ch/en/publication/7029

[13] Automation Security Management in the Process Industry – NA 169
Autor: NAMUR

[14] DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis
Author: EC Council
Link: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/

[15] The threats to our products
Author: L. Kohnfelder and P. Garg
Microsoft Interface, April 1999

[16] The Purdue Enterprise Reference Architecture
Author: T.J. Williams
Computers in industry Vol 24, 1994

[17] The Industrial Internet Reference Architecture
Author: Industrial Internet Consortium
Link: https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf

[18] IEC Common Data Dictionary
Author: IEC TC 3
Link: https://cdd.iec.ch/

Version history

Version	Date	Changes
Version 01.00	April 2026	Release of version 1.00

FieldComm Group

fieldcommgroup.org

ODVA

odva.org

OPC Foundation

opcfoundation.org

Profibus and Profinet International (PI)

profibus.com