IO-Link Secure Deployment Guideline

Guideline

V1.0.0

June 2025

Order No: 10.502

File name: **IO-Link-SecureDeploymentGuideline_10502_V100_Jun25.pdf**

This document has been prepared, approved, and released by the IO-Link Coreteam in collaboration with security experts.

Any comments, proposals, requests on this document are appreciated. Please use www.io-link-projects.com for your entries and provide name and email address.
Login: **IO-Link-Security**
Password: **Report**

Publisher:
IO-Link Community
c/o PROFIBUS Nutzerorganisation e.V.
Ohiostrasse 8
76149 Karlsruhe
Germany
Phone: +49 721 / 98 61 97 0
Fax: +49 721 / 98 61 97 11
E-mail: info@io-link.com
Web site: www.io-link.com

LICENSE AGREEMENT

1. License

1.1 Subject of this license agreement is this document issued by the Licensor, in electronic form. If applicable, also software may be provided.

1.2 The user of this document (Licensee) acquires the license solely from PROFIBUS Nutzerorganisation e.V., having its principal place of business in Karlsruhe, Germany (hereinafter referred to as “Licensor”).

1.3 This document is not an industrial standard acknowledged by any standardization body or otherwise and may be further enhanced.

2. Rights and Duties of Licensee

2.1 Licensor hereby grants to Licensee the right to use this document exclusively for developing and supporting products compliant with this document. Licensee may copy this document for this purpose and for data backup purposes.

2.2 Licensee shall not be entitled to modify, decompile, reverse engineer or extract any individual parts of this document, unless this is permitted by mandatory Copyright Law. Furthermore, Licensee shall not be entitled to remove any alphanumeric identifiers, trademarks or copyright notices from this document and, insofar as Licensee is entitled to make copies of this document, Licensee shall copy them without alteration.

2.3 Licensee is not entitled to copy and redistribute this document to any third party, except for “Have Made” purposes. All copies must be obtained on an individual basis, directly from the website www.profibus.com or upon request from the Licensor.

2.4. Licensee agrees to comply with all applicable export control, trade, and sanctions regulations as well as embargo regulations of the European Union, the United States of America, and other relevant jurisdictions (“Export Control Regulations”). This applies in particular to the applicable Export Control Regulations relating to Russia and Belarus and with natural or legal persons associated with Russia and Belarus. Should Licensor become aware of any violation of Export Control Regulations with respect to the use of this document, PNO reserves the right to terminate this Agreement without notice and claim damages.

3. Liability of Licensor

3.1 Licensor shall have no obligation to enhance the document and shall assume no liability in case the document or future versions thereof shall not be approved as an industrial standard.

3.2 Licensor’s liability for defects as to quality or title of this document, especially in relation to the correctness or absence of defects or the absence of claims or third-party rights or in relation to completeness, usability and/or fitness for purpose are excluded, except for cases involving gross negligence, willful misconduct or fraudulent concealment of a defect.

3.3 Any further liability is excluded unless required by law, e.g. in cases of personal injury or death, willful misconduct, gross negligence, or in case of breach of fundamental contractual obligations. The damages in case of breach of fundamental contractual obligations is limited to the contract-typical, foreseeable damage if there is no willful misconduct or gross negligence.

4. Place of Jurisdiction and Applicable Law

4.1 The sole place of jurisdiction shall be the principal place of business of Licensor.

4.2 All relations arising out of the contract shall be governed by the substantive law of Germany, to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG).

Conventions:

In this specification the following key words (in **bold** text) will be used:

shall:	indicates a mandatory requirement. Designers shall implement such mandatory requirements to ensure interoperability and to claim conformity with this specification.
should:	indicates flexibility of choice with a strongly preferred implementation.
can:	indicates flexibility of choice with no implied preference (possibility and capability).
may:	indicates a permission.
highly recommended:	indicates that a feature shall be implemented except for well-founded cases. Vendor shall document the deviation within the user manual and within the manufacturer declaration.

CONTENTS

0 Introduction

0.1 General

The base technology of IO-Link™[1] is subject matter of the international standard IEC 61131-9 (www.iec.ch). IEC 61131-9 is part of a series of standards on programmable controllers and the associated peripherals and should be read in conjunction with other parts of the series.

IO-Link is a wired point-to-point digital communications technology that allows low-cost sensors and actuators to exchange the diagnosis and configuration data with a controller while maintaining compatibility with traditional discrete signalling.

IO-Link Devices are deployed in different industries and in a variety of physical environments.

The main purpose of IO-Link Devices is to detect physical properties and pass them on to the controlling system using digital signals. In addition to digital signal transmission, the IO-Link technology enables self-description of assets. IO-Link Device access and parameterization are done using the IO-Link interface by other components (PLCs, IO-Link Masters, etc.) that can be physically co-located with the device itself.

0.2 Disclaimer

Due to the constantly changing nature of the security landscape and mounting threats on Industrial Automation and Control Systems, the laws, standards and interpretations are constantly evolving, and new documents are added as new topics arise. In parallel, a joint working group is developing a common view on comparable protocol standards to harmonize the industrial view in a broader sense.

If necessary, new versions of this document will be derived on the base of this new aspects.

1 Motivation and scope

Recent emphasis on cybersecurity in the Industrial Automation Systems (IACS) created a need to establish a security approach to installing and operating IO-Link devices, which this guide is attempting to address.

The security discussion is based on IEC 62443, a series of documents that cover multiple security aspects of IACS.

The scope of this guide is IO-Link communication over a wired connection according to IEC 61131-9:2022 that represents current state-of-the-art communications technology for low-cost field devices.

IO-Link is a wired point-to-point protocol that does not provide any networking functions and does not incorporate Ethernet, TCP/IP, or any other network features that include routing or addressing.

The focus of this guide is therefore defined as the wired point-to-point protocol that IO-Link is, and the devices that use IO-Link to communicate with their masters. This is illustrated in Figure 1.

---

[1] IO-Link™ is a trade name of the "IO-Link Community". This information is given for the convenience of users of this specification and does not constitute an endorsement by the "IO-Link Community" of the trade name holder or any of its products. Compliance to this standard does not require use of the registered logos for IO-LinkTM. Use of the registered logos for IO-Link™ requires permission of the "IO-Link Community".

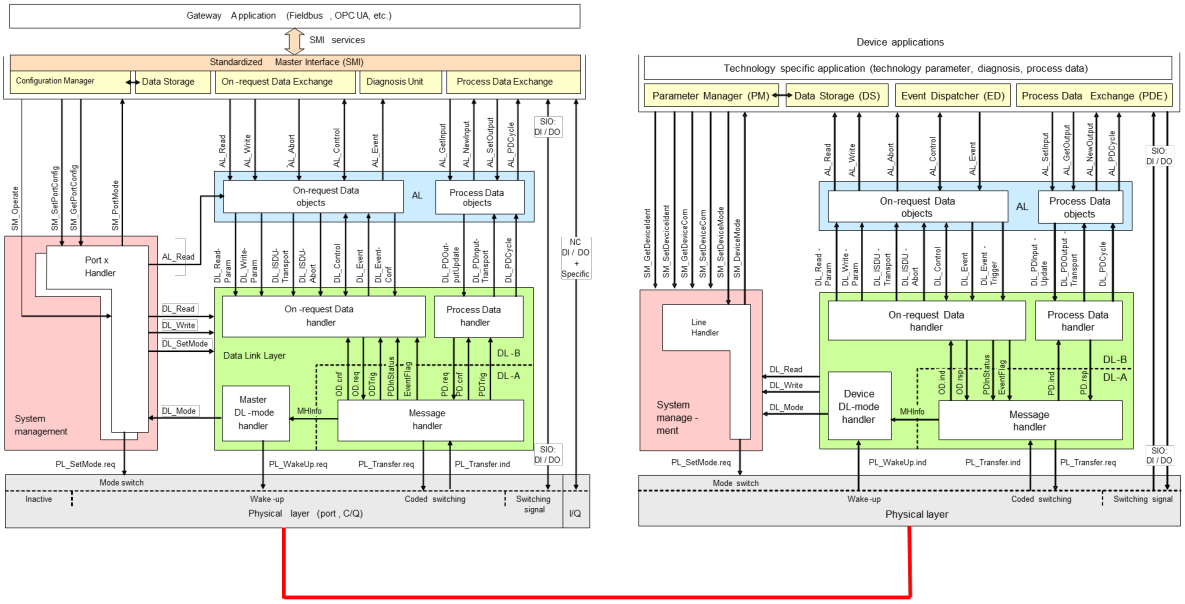

Figure 1 – IO-Link Physical Protocol

Even though some IO-Link Devices can have local functionality for user interaction, this functionality is not included in the scope of this document. Also not included in the scope of this document are any infrastructure devices that can be placed between IO-Link Master and IO-Link Device and that may inadvertently enable data sniffing or impact data confidentiality.

This document covers IO-Link Interface Specification V1.1.3 and is also applicable to V1.1.4.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61131-9:2022, *Programmable controllers - Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI), IO-Link V1.1.3*

IO-Link Community, *IO-Link Interface and System Specification, V1.1.4*

IEC 61443-1-1:2009, *Terminology, concepts and models*

IEC 62443-3-2:2020, *Security Risk Assessment for system design*

IEC 62443-3-3:2019, *System security requirements and security levels*

IEC 62443-4-1:2018, *Secure product development lifecycle requirements*

IEC 62443-4-2:2019, *Technical security requirements for IACS components*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Common terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61131-1 and IEC 61131-2, as well as the following apply.

3.1.1
Asset
physical or logical object owned by the organization, typically the equipment under control

3.1.2
Attack
a deliberate attempt to violate security policy of the system

3.1.3
Conduit
logical grouping of communications assets that protects the security of the channels it contains

3.1.4
Data confidentiality
Property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities or processes

3.1.5
IACS
Industrial Automation and Control Systems

3.1.6
Outsider
person or group not trusted with inside access

3.1.7
Penetration
successful unauthorized access to a protected system resource

3.1.8
Security Zone
grouping of logical or physical assets that share common security requirements

3.1.9
Sniffing
capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communications system. In the specific case of IO-Link, sniffing attack could occur only if an outsider successfully penetrated physical security zone where IO-Link system is deployed.

3.1.10
Point-to-point
private data connection securely connecting two locations, typically over a dedicated physical link

4 Security Analysis

4.1 IACS Security Environment for IO-Link Devices

IO-Link is intended for operation in logically and physically secure zones defined by the customer (system integrators and asset owners).

Based on the reference model for IEC 62443 standards provided in IEC 62443-1-1:2009 (section 6.2.1) [3], IO-Link Devices are installed and operated at level 0 (Process Level). This is illustrated in Figure 2 below.

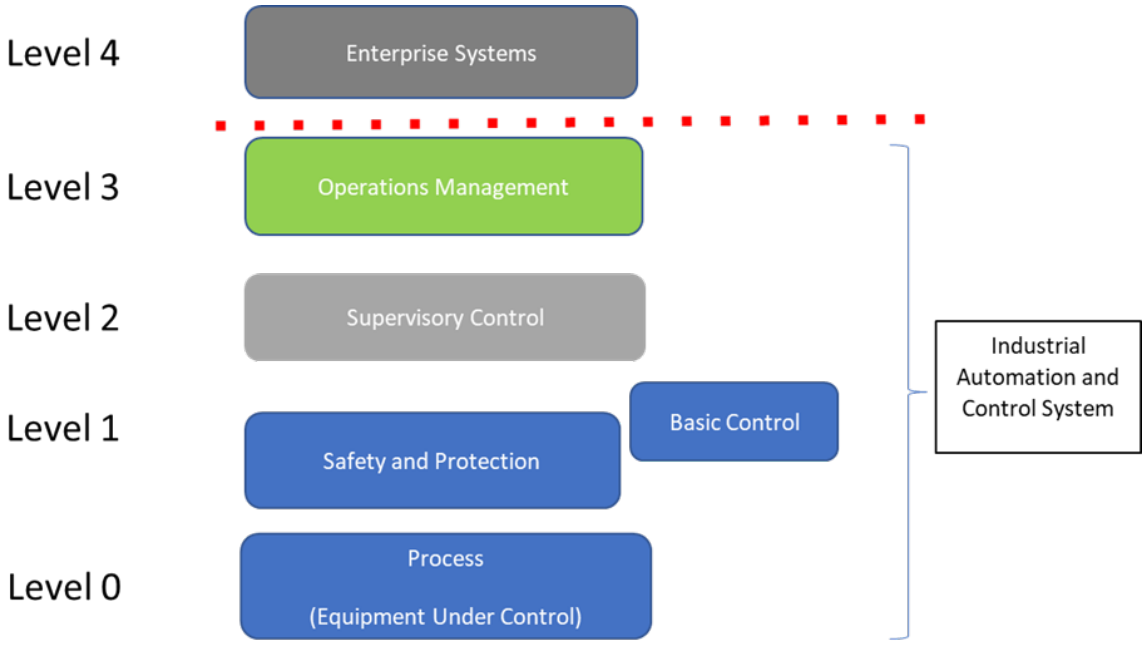

Figure 2 – IEC 62443 Reference Model

At Level 0, IO-Link Devices and IO-Link communication links are locally restricted. IO-Link Devices are not directly accessible outside of the deployment security zone through any of the security conduits to the zone.

Security of IO-Link Devices and IO-Link communications relies on physically securing IO-Link communications link and physically limiting access to IO-Link Devices within the zone.

During installation, access to the physical plant (IO-Link cable and its cable connection) needs to be analysed. If the cable or cable connection to the device poses a security risk, the physical plant needs to be physically secured. The same approach should be applied to the installation of the IO-Link Device itself.

Physical security of IO-Link Devices and the IO-Link physical plant must be covered by security policies established by the customer and verified by performing the risk analysis of the IACS system, per IEC 62443-1-1:2009 section 5.8.4.5 [3].

4.2 Threat Model

The IO-Link Device and interface threat model is available in **"Secure design and development guideline for IO-Link Devices"** [8], a separate document published by the IO-Link Community.

NOTE: The "Secure design and development guideline for IO-Link Devices" is in progress and planned to be released in 2025

4.3 Security capabilities of IO-Link Devices

The security capabilities assume that all IO-Link Devices comply with the requirements described in the "Secure design and development guideline for IO-Link Devices" [8].

Due to the definition of the communication relationship between the IO-Link Device and the IO-Link Master, the needed security requirements are restricted to a limited scope of threats.

According to the intended use, the protocol specific restrictions, the primary protection targets are the availability and the integrity of the system itself and the sensor data.

Based on the specific properties of the IO-Link protocol, IO-Link Devices are classified as "embedded devices" according to IEC EN 62443-4-2 Annex A.2 [7].

According to the "foundational requirements" listed in IEC EN 62443-1-1 section 5.3 [3], IO-Link Devices are restricted but not limited to the following protection targets:

Table 1 – Protection Targets

Protection target	Impact / Risk	Rationale
Identification and authentication control (IAC)	LOW / not applicable	Limited or no human interaction with IO-Link Device
Use control (UC)	LOW / not applicable	Due to the lack of user authentication, no authorization is carried out within the IO-Link protocol
System Integrity (SI)	High	System integrity and Data Integrity are pre-defined primary protection goals.
Data confidentiality (DC)	LOW / not applicable	Data confidentiality can be impacted if outsider can gain physical access to the point-to-point link and physically attach very specialized equipment. Due to the skill set and equipment needed to achieve this, the security impact and risk are deemed to be low. Due to the absence of data protection features (encryption), no data confidentiality features are available within the IO-Link protocol.
Restricted Data flow (RDF)	LOW / not applicable	Due to the protocol specific point-to-point communication relationship, there are no security concerns
Timely response to events (TRE)	LOW / not applicable	Due to the protocol specific point-to-point communication relationship, there are no security concerns
Resource availability (RA)	High	Resource availability can be impacted by disrupting the physical connection or rendering the IO-Link Device unusable

4.4 Conclusion

4.4.1 Limitations of the IO-Link protocol

In general, current implementations of IO-Link protocol do not provide common security features that are typically present in network protocols, such as:

- Device Authentication
- User Authorization
- Data Encryption

However, viewed from specific IO-Link perspective, the given point-to-point nature of the wired IO-Link protocol, the risk associated with the absence of these features is minimal to non-existent.

4.4.2 Main threats in deployment of wired IO-Link devices

After extensive discussions, as threats that have been identified with deployment of wired IO-Link devices are only related to

- IO-Link Device availability
- Sniffing
- Data tampering

All the items in this list can only be achieved if physical security is breached, and direct physical access is obtained to either the cable carrying IO-Link protocol or the actual IO-Link Device. Sniffing and data tampering require highly specialized technical skills and access to specialized equipment, placing them beyond Security Level 2, as defined in IEC 62443-3-3:2019 Annex A [5]. It is also highly likely that any attempt at sniffing and/or data tampering will impact IO-Link Device availability, which is readily detectable in the properly configured IACS.

4.4.3 Recommendations for security

Security recommendations for zoning and security audits (per 62443-2) must be followed to maintain the security posture of the deployed system.

The following IO-Link-specific recommendations must be considered:

1) The IO-Link protocol does not provide encryption. If you come to the conclusion in your risk assessment that you need to protect the confidentiality of the IO-Link communication, then we recommend to restrict physical access to the IO-Link cable and the IO-Link Device.
2) The IO-Link protocol does not provide authenticity or integrity protection (except for the CRC). If you come to the conclusion in your risk assessment that you need (higher) protection of the authenticity or integrity of the IO-Link communication, then we recommend to restrict physical access to the IO-Link cable and to the IO-Link Device.
3) The IO-Link protocol does not provide access control. If you come to the conclusion in your risk assessment that you need access control to prevent unauthorized users from interacting with the IO-Link Device, then we recommend that you implement/configure access control in the system by other means (e.g., physical access protection).
4) We recommend to monitor the events the IO-Link Device reports to the IO-Link Master and to take appropriate actions, where necessary (e.g., replace a faulty IO-Link Device).
5) According to the IO-Link Community, it is recommended to back up the settings of the IO-Link Device using the Master with the backup levels 'Backup&Restore' or 'Restore', and to test the procedure for restoring the settings of IO-Link Devices.
6) In case of reported security issues of an IO-Link Device please follow the manufacturer recommendations.

182

183 # Bibliography

184 [1] IEC 61131-9:2022, *Programmable controllers - Part 9: Single-drop digital*
185 *communication interface for small sensors and actuators (SDCI), IO-Link V1.1.3*

186 [2] IO-Link Community, *IO-Link Interface and System Specification, V1.1.4*

187 [3] IEC 61443-1-1:2009, *Terminology, concepts and models*

188 [4] IEC 62443-3-2:2020, *Security Risk Assessment for system design*

189 [5] IEC 62443-3-3:2019, *System security requirements and security levels*

190 [6] IEC 62443-4-1:2018, *Secure product development lifecycle requirements*

191 [7] IEC 62443-4-2:2019, *Technical security requirements for IACS components*

192 [8] IO-Link Community, *Secure design and development guideline for IO-Link Devices*
193 *(under development)*

194 _____

195

IO-Link Community
c/o PROFIBUS Nutzerorganisation e.V.

Ohiostrasse 8
76149 Karlsruhe
Germany
Phone: +49 (0) 721 / 98 61 97 0
Fax: +49 (0) 721 / 98 61 97 11
e-mail: info@io-link.com
Web site: www.io-link.com/