

IO-Link Secure Deployment Guideline

Guideline

Draft 0.9.3

December 2024

Order No: 10.502

File name: **IO-Link-SecurityDeploymentGuideline_10502_Current.docx**

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

This document is for review until February 28th, 2025.

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**

NOTICE:


The information contained in this document is subject to change without notice. The material in this document details a PNO specification in accordance with the license and notices set forth on this page. This document does not represent a commitment to implement any portion of a PNO specification in any company's products.

The attention of adopters is directed to the possibility that compliance with or adoption of PNO specifications may require use of an invention covered by patent rights. PNO shall not be responsible for identifying patents for which a license may be required by any PNO specification, or for conducting legal inquiries into the legal validity or scope of those patents that are brought to its attention. PNO specifications are prospective and advisory only. Prospective users are responsible for protecting themselves against liability for infringement of patents.

WHILE THE INFORMATION IN THIS DOCUMENT IS BELIEVED TO BE ACCURATE, PNO MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS DOCUMENT INCLUDING, BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, IMPLIED WARRANTY OF MERCHANTABILITY OR WARRANTY OF FITNESS FOR PARTICULAR PURPOSE OR USE.

In no event shall PNO be liable for errors contained herein or for indirect, incidental, special, consequential, reliance or cover damages, including loss of profits, revenue, data or use, incurred by any user or any third party. Compliance with PNO specifications does not absolve manufacturers, from the requirements of safety and regulatory agencies (TÜV, BIA, UL, CSA, etc.).

USE OF TRADEMARKS:

 **IO-Link** ® is registered trade mark. The use is restricted for members of the IO-Link Community. More detailed terms for the use can be found in the IO-Link Community Rules on www.io-link.com.

PNO is the owner of several registered trademarks, such as PROFIBUS®, PROFINET®, omlox®, IO-Link®, MTP® and others. More detailed terms for the use can be found on the web page www.profibus.com. Please select buttons "Downloads / Presentations & logos". In some cases, PNO is the licensee of registered trademarks owned by third parties and which may be relevant in regard with products compliant to this document.

PNO shall always be the sole entity that may authorize developers, suppliers and sellers of hardware and software to use certification marks, trademarks or other special designations to indicate compliance with a PNO specification. Products developed using a PNO specification may claim compliance or conformance with a PNO specification only if the hardware and/or software satisfactorily meets the certification requirements set by PNO. Products that do not meet these requirements may claim only that the product was based on a PNO specification and must not claim compliance or conformance with a PNO specification.

COPYRIGHT

Copyright © 2024 PROFIBUS Nutzerorganisation e.V.

Any unauthorized use of this publication may violate Copyright Law, Trademark Law and other legal regulations. This document contains information which is protected by Copyright. No part of this work covered by Copyright herein may be reproduced or used in any form or by any means -graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems--without permission of the publisher.

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.de.profibus.com or www.profibus.com or upon request from the Licensor.

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, wilful 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, wilful 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 wilful 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 Introduction5
- 0.1 General5
- 1 Motivation and scope.....5
- 2 Normative references6
- 3 Terms, definitions, symbols, abbreviated terms and conventions6
- 3.1 Common terms and definitions6
- 4 Security Analysis7
- 4.1 IACS Security Environment for IO-Link Devices7
- 4.2 Threat Model8
- 4.3 Security capabilities of devices8
- 4.4 Conclusion10
- Bibliography.....11

- Figure 1 – IO-Link Physical Protocol6
- Figure 2 – IEC 62443 Reference Model8

- Table 1 – Protection Targets9

1 0 Introduction

2 0.1 General

3 The base technology of IO-Link^{TM1} is subject matter of the international standard IEC 61131-9
4 (www.iec.ch). IEC 61131-9 is part of a series of standards on programmable controllers and the
5 associated peripherals and should be read in conjunction with other parts of the series.

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

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

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

15

16 1 Motivation and scope

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

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

22 The scope of this guide is IO-Link communication over a wired connection according to IEC
23 61131-9:2022 that represents current state-of-the-art communications technology for low-cost
24 field devices.

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

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

¹ IO-LinkTM 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-LinkTM requires permission of the "IO-Link Community".

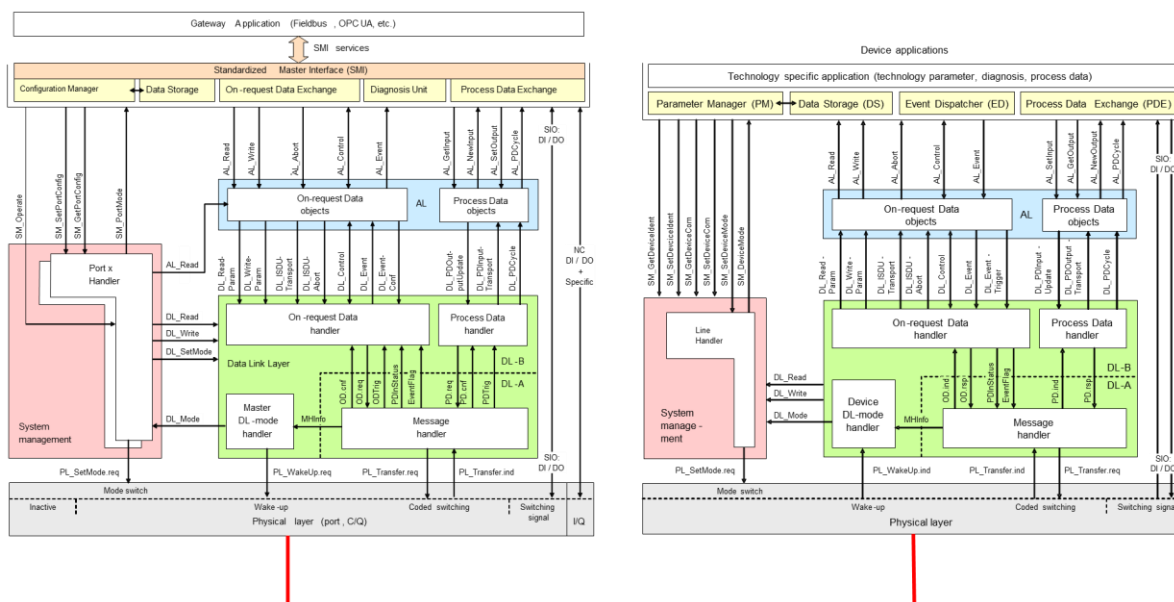


Figure 1 – IO-Link Physical Protocol

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

57 3.1.2**58 Attack**

59 a deliberate attempt to violate security policy of the system

60 3.1.3**61 Conduit**

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

63 3.1.4**64 Data confidentiality**

65 Property that information is not made available or disclosed to any unauthorized system entity,
66 including unauthorized individuals, entities or processes

67 3.1.5**68 IACS**

69 Industrial Automation and Control Systems

70 3.1.6**71 Outsider**

72 person or group not trusted with inside access

73 3.1.7**74 Penetration**

75 successful unauthorized access to a protected system resource

76 3.1.8**77 Security Zone**

78 grouping of logical or physical assets that share common security requirements

79 3.1.9**80 Sniffing**

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

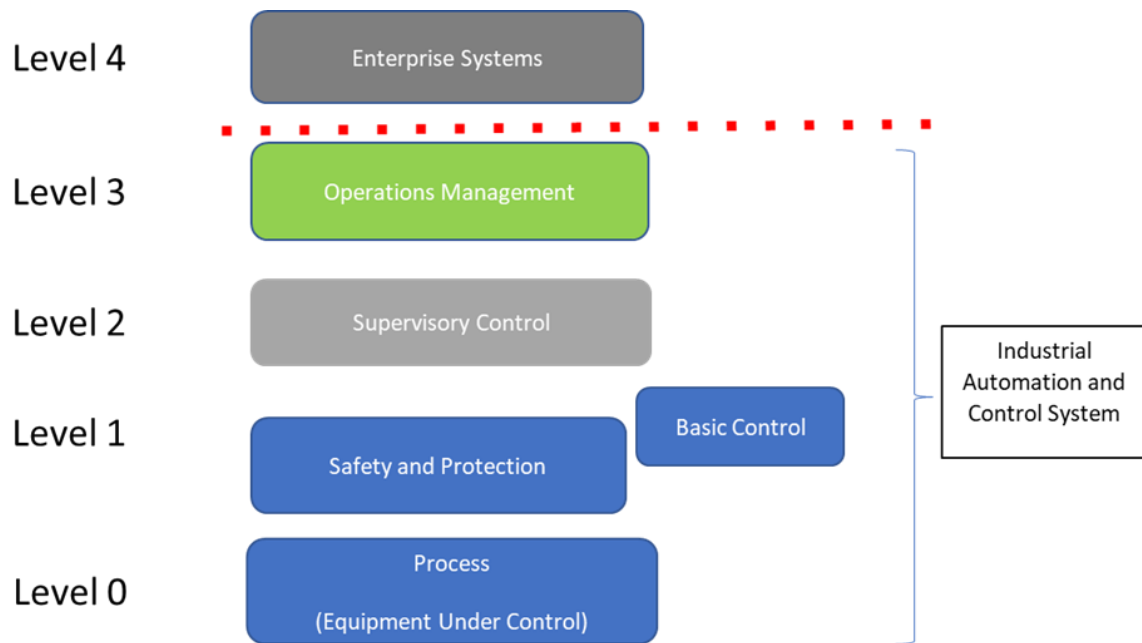
85 3.1.10**86 Point-to-point**

87 private data connection securely connecting two locations, typically over a dedicated physical
88 link

89 4 Security Analysis**90 4.1 IACS Security Environment for IO-Link Devices**

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

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



96
97 **Figure 2 – IEC 62443 Reference Model**

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

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

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

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

110 4.2 Threat Model

111 IO-Link device and interface threat model is available in “**Secure design and development
112 guideline for IO-Link Devices**” [8], a separate document published by IO-Link Community.

113 NOTE: This document is in progress is planned to be released in 2025

114 4.3 Security capabilities of devices

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

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

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

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

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

125

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 lack of data protection features (encryption), no data confidentiality features are available within 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

126

127 **4.4 Conclusion**

128 Current implementation of IO-Link protocol lacks common security features that are typically
129 present in networked protocols, such as:

- 130 • Device Authentication
- 131 • User Authorization
- 132 • Data Encryption

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

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

- 137 • IO-Link device availability
- 138 • Sniffing
- 139 • Data tampering

140 All the items in this list can only be achieved if physical security is breached, and direct physical
141 access is obtained to either the cable carrying IO-Link protocol or the actual IO-Link device.
142 Sniffing and data tampering require highly specialized technical skills and access to specialized
143 equipment, placing them beyond Security Level 2, as defined in IEC 62443-3-3:2019 Annex A
144 [5]. It is also highly likely that any attempt at sniffing and/or data tampering will impact IO-Link
145 device availability, which is readily detectable in the properly configured IOCS.

146 If security concerns are present, limiting physical access to IO-Link device and associated cable
147 can be used as an effective means to address the immediate security needs.

148 In addition, security recommendations for zoning and security audits (per 62443-2) must be
149 followed to maintain the security posture of the deployed system.

150

151

152

Bibliography

153

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

154

155

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

156

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

157

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

158

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

159

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

160

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

161

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

162

163

164

© Copyright by:

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/



IO-Link