IO-Link Security Design and Development

Guideline

D1.0.0-01
October 2025

Order No: 10.512

File name:
IOL_Security_Des&Dev_Guideline_10512_D1.0.0-01_Oct2025.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 03, 2026.
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

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 signaling.

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

To design and develop IO-Link devices it is necessary to fulfill several different requirements. One important aspect is security: as emerges from laws (e.g., EU CRA, US cybersecurity executive order) and standards (e.g. IEC 62443) from around the world there is an increasing demand for security in depth approaches for connected systems and devices with digital elements in general.

Specifically in the context of IO-Link Devices the community works on two different levels:

- Deployment: The outside perspective of the Devices: the IO-Link protocol and the Devices as black boxes, handled in the guideline "IO-Link Secure Deployment Guideline".
- Design and Development; The development rules are handled of Devices is handled in this document.

The Scope of this document is IO-Link communication via a wired connection according to IO-Link Interface and System Specification [2] that represents current state-of-the-art. IO-Link is a point-to-point protocol that does not provide any networking functions and does not incorporate either Ethernet or TCP/IP functionalities.

Based on the specific properties of the IO-Link protocol and IO-Link devices, these are summarized as "embedded devices" according to definition in IEC EN 62443-4-2. The main purpose of IO-Link is to detect physical properties and pass them on via electrical signals.

---

[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".

This document describes the security measures that must be implemented to fulfill the technical security requirements of IEC 62443-4-2 for reaching security level SL-C 1 by a simple IO-Link Device.

In addition to digital signal transmission, IO-Link enables the self-description of assets. Access and parameterization are done via the IO-Link interface, via other devices above or directly local at the device itself.

In this document, we explicitly define the scope as the point-to-point protocol that IO-Link is, and the Devices that use IO-Link to communicate with their Masters, where the Devices offer no possibility of local user interaction (buttons, display, wireless, ...), other than the IO-Link connection itself. Figure 1 shows the red dot boxed area of the scope of this document.

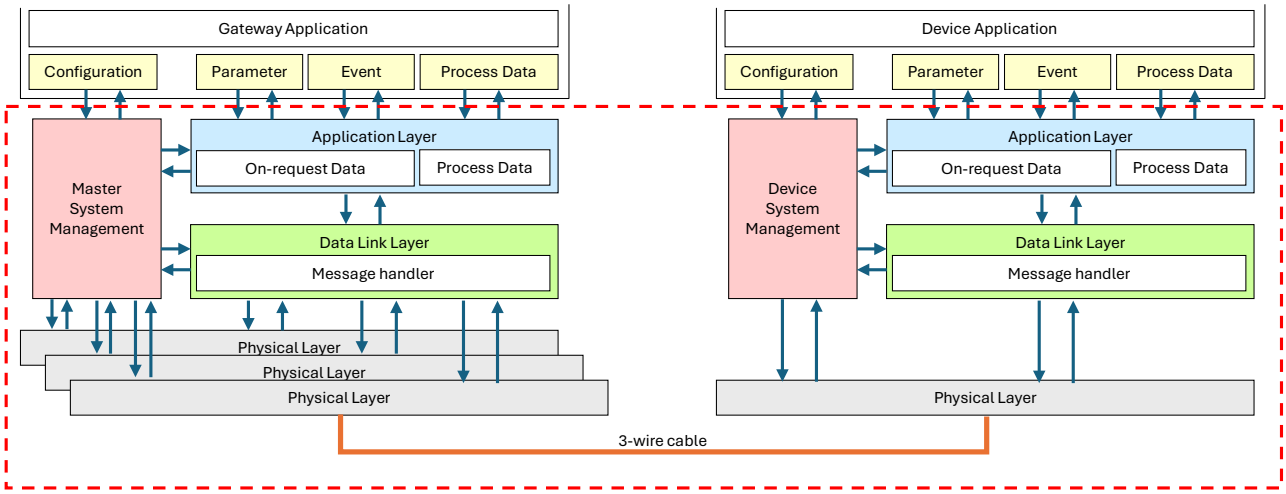

Figure 1 – IO-Link physical protocol compartment

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IO-Link Interface and System Specification V1.1.5 or higher

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, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62443 series, IO-Link Interface and System Specification, and the following apply.

For easy reading, the following important terms are copied from the sourcing documents.

3.1.1 Device

single passive peer to a Master such as a sensor or actuator

Note 1 to entry: Uppercase "Device" is used for SDCI equipment, while lowercase "device" is used in a generic manner.

3.1.2 Master

active peer connected through ports to one up to n Devices and which provides an interface to the gateway to the upper level communication systems or PLCs

Note 1 to entry: Uppercase "Master" is used for SDCI equipment, while lowercase "master" is used in a generic manner.

3.2 Symbols and abbreviated terms

CRC	Cyclic redundancy check
EU-CRA	European Union – Cyber Resilience Act
IACS	industrial automation and control system(s)
SL-C	capability security level
STRIDE	Spoofing, Tampering, Repudiation, Information of disclosure, Denials of service, Elevation of privilege
FR	Functional requirement according IEC 62443-4-2

4 Relation to standards, norms and laws

4.1 IEC 62443 IACS Cybersecurity Standards

This guideline document is aligned with and based on IEC 62443 IACS Cybersecurity Standards. IEC 62443 is divided into multiple parts (documents) that cover the following areas:

- General security models and concepts (IEC 62443-1 series),
- Policies and Procedures for asset owners and IACS service providers (IEC 62443-2 series)
- System security considerations, requirements, and security levels (IEC 62443-3 series)
- Component security development lifecycle and technical requirements (IEC 62443-4 series)

Due to the constantly changing nature of the security landscape and mounting threats on IACS systems, IEC 62443 standard is constantly evolving, and new documents are added as new topics arise. The standard presently consists of 14 parts, as shown in Figure 2.

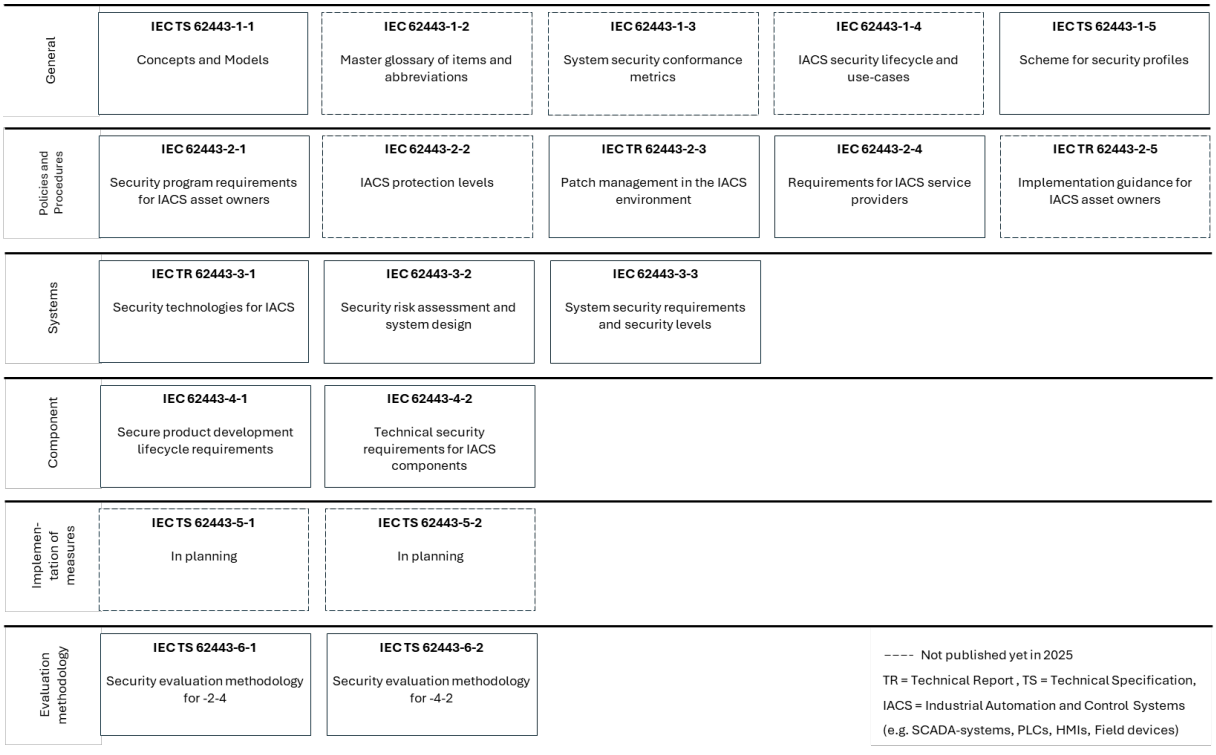

Figure 2 – Overview of IEC 62443 series

It should be noted that the IEC 62443 standard is centered around Ethernet and TCP/IP based networks. It does not address security considerations for non-Ethernet and non-TCP communication systems that are also common in today's industrial installations. Examples of such systems include IO-Link, PROFIBUS, DeviceNet, and others.

4.2 Laws

The laws around the world are varying heavily and evolve in different ways – thus we do not focus on any specific law in the context of the IO-Link security documents.

Developers shall refer to the relevant laws and regulations that apply for specific use cases and countries.

For a reference of applicable laws known to the authors of this document please refer to the list in Annex A.

4.3 Purpose of this document on design and development

The purpose of this document is to provide Device manufacturers with IO-Link Community recommendations for their respective product Security Development Guidelines, based on aspects derived from the standards.

Authors of this guideline document rely primarily on the document "IO-Link Security Deployment Guideline" and IEC Parts 62443-4-1 and 62443-4-2 to recommend device security implementations.

4.4 IO-Link and Security

Please read the document "IO-Link Security Deployment Guideline".

4.5 Security Levels

Please read the document "Security Deployment Guide for IO-Link Devices".

From that document we identified the need to achieve a basic level of security in the implementation of Devices.

5 Recommendations for design and development of Devices

The following IO-Link communication features are well-known

- The IO-Link interface and communication protocol features cable-bound, point-to-point, half-duplex communication via 24 V digital I/Os
- Checksum protection on message level
- CRC protection on data package level
- As of now, it is quite usual to secure IO-Link Devices by physical means. Nonetheless secure development and deployment aspects should be considered to enable security-in-depth by raising the overall security bar and reducing the chances of accidental or intentional tampering / interference

Specific recommendations for developing, integrating and supporting systems are relevant:

- Focus on System and Software, Hardware is irrelevant at this stage
- Overall system requirements need to consider the relevant information from the document "IO-Link Security Deployment Guideline".
- Some devices might come with a user interface (Display, Buttons, ...). The IO-Link system provides a standardized way for disabling the user interface, we recommend to implement this option to lock the user interface to reduce the chances of changing device settings or compromising device functionality by accidentally interacting with the device locally, without the system administrators being involved

– IEC 62443-4-1 recommends a Secure Development Lifecycle (SDL) to be put in place and lived by: security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life.

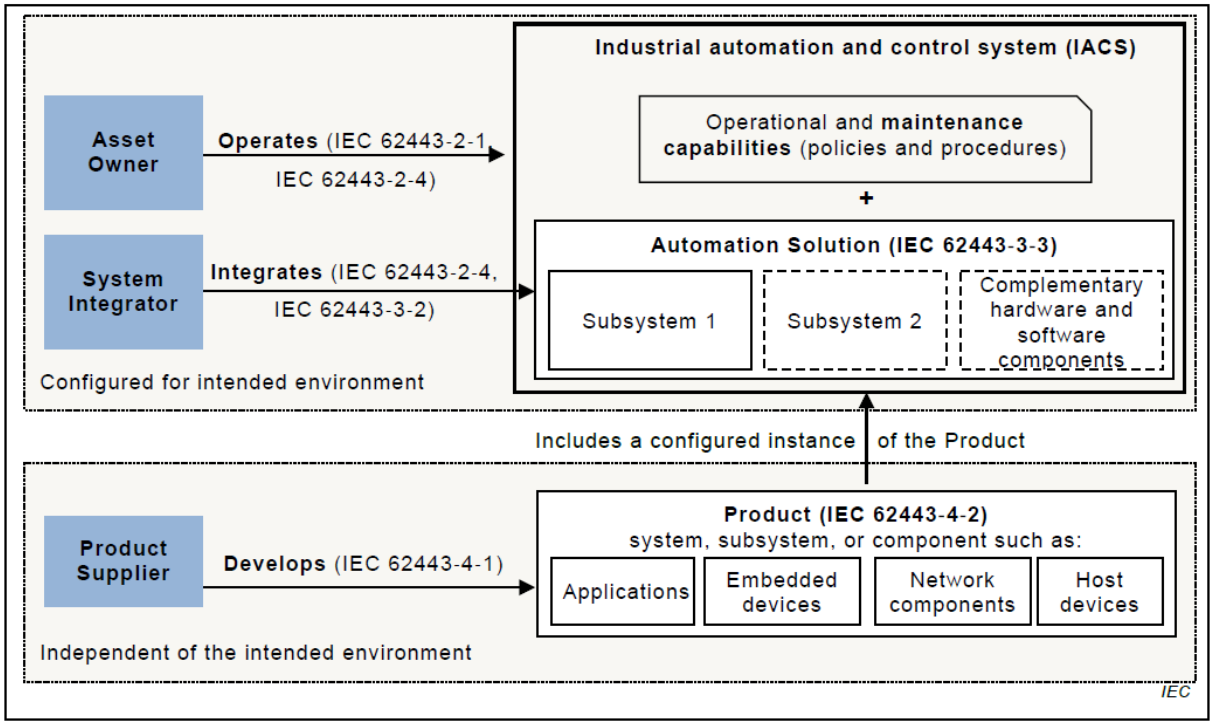

Figure 3 – Example scope of product life-cycle

6 Threat-Modeling

Based on the topology considered in the context of this consideration (see 1) and the consideration of STRIDE methodology, the following threats are identified on the basis of the corresponding attacker motivation and the associated impact, and suitable countermeasures are presented.

Motivation: Potential attackers intend to negatively influence the application's value-added process. This requires elementary knowledge of the application, and the products used.

Impact: Application availability and quality of the value creation process.

Table 1 lists the considered threats. Each threat is described with the related thread type, interface, impact and recommended counter measures

156 **Table 1 – Thread model and implications**

Threat	Threat Typ	Interface	Impact	Countermeasure
Attacker can pretend to be the "correct" IO-Link Device to the IO-Link Master, but behave maliciously, e.g. send wrong sensor data to the Master	Spoofing	Wired connection IO-Link cable, physical device	Actuator commands Parameter modification During runtime At commissioning time of the Device Changed dataset in the Master by a malicious Device Authenticity of Device without malicious intention Spoofing data for another Device connected to another port? Addressing wrong Device / Master as intended – verification of authenticity	Physical protection of communication cable and devices
Attacker can pretend to be the "correct" IO-Link Master to the IO-Link Device, but behave maliciously, e.g. send wrong actuator commands or configuration settings to the Device	Spoofing	Wired connection IO-Link cable; Device		Physical protection of communication cable and devices
Attacker can modify, replay previously recorded and insert forged messages in both communication directions, e.g. send wrong data, send wrong configuration settings, send invalid messages	Tampering	Wired connection IO-Link cable	Changing IODD contents to allow formally forbidden actions, tampering IODDs	Physical protection of communication cable and devices
Attacker can record all messages and disclose them to unauthorized parties	Information disclosure	Wired connection IO-Link cable		Physical protection of communication cable and devices
Attacker can disconnect Master and Device at any time Attacker can selectively delete messages in both communication directions Attacker can send large amounts of valid or invalid messages to IO-Link Master or Device in order to overload or crash them	Denial of service	Wired connection IO-Link cable, physical device		Physical protection of communication cable and devices

157

158 # 7 Overview of functional requirements

159 ## 7.1 General

160 Based on the result of the threat analysis and the intended use, the following technical require-
161 ments based on fundamental requirements (see IEC 62443-1-1) are recommended.

162 As IO-Link Devices are expected to be used in SL-C 1 environment only, the following interpre-
163 tation is focused on SL-C 1 requirements.

164 This clause describes the technical requirement for each functional requirement according IEC
165 62443-4-2:2019, further information on this may be obtained there.

166 The results are shown in Table 2 as an overview with assessed relevance. The following
167 clauses contain detailed description for each requirement with justification or contextual map-
168 ping.

169 **Table 2 – IEC 62443 related requirements**

Category	Requirement	Relevant	Details
FR 1 – Identification and Authentication Control	CR 1.1 – Human user identification and authentication	no	7.2.2
	CR 1.3 – Account Management	no	7.2.3
	CR 1.4 – Identifier Management	no	7.2.4
	CR 1.5 – Authenticator Management	no	7.2.5
	CR 1.7 – Strength of password-based authentication	no	7.2.6
	CR 1.10 – Authenticator Feedback	no	7.2.7
	CR 1.11 – Unsuccessful Login Attempts	no	7.2.8
	CR 1.12 – System Use Notifications	no	7.2.9
FR 2 – Use Control	CR 2.1 – Authorization Enforcement	no	7.3.2
	CR 2.2 – Wireless use control	no	7.3.3
	CR 2.5 – Session lock	no	7.3.4
	CR 2.8 – Auditable Events	yes	7.3.5
	CR 2.9 – Audit storage capacity	yes	7.3.6
	CR 2.10 – Response to Audit Processing Failures	yes	7.3.7
	CR 2.11 – Timestamps	no	7.3.8
	CR 2.12 – Non-repudiation	no	7.3.9
FR 3 – System Integrity	CR 3.1 – Communication Integrity	yes	7.4.2
	CR 3.3 – Security functionality verification	yes	7.4.3
	CR 3.4 – Software and information integrity	yes	7.4.4
	CR 3.5 – Input Validation	yes	7.4.5
	CR 3.6 – Deterministic Output	yes	7.4.6
	CR 3.7 – Error Handling	yes	7.4.7
FR 4 – Data Confidentiality	CR 4.1 – Information Confidentiality	yes	7.5.2
	CR 4.3 – Use of cryptography	yes	7.5.3
FR 5 – Restricted Data Flow	CR 5.1 – Support Network Segmentation	yes	7.6.2
FR 6 – Timely response to events	CR 6.1 – Audit log accessibility	no	7.7.2
FR 7 – Resource Availability	CR 7.1 – Denial of Service Protection	no	7.8.2
	CR 7.2 – Resource Management	no	7.8.3
	CR 7.3 – Control System Backup	yes	7.8.4
	CR 7.4 – Control system recovery and reconstitution	yes	7.8.5
	CR 7.6 – Network and security configuration settings	yes	7.8.6
	CR 7.7 – Least Functionality	yes	7.8.7
Software Application Requirements	SAR 2.4 – Mobile Code	no	7.9.2
	SAR 3.2 – Protection from malicious code	no	7.9.3
Embedded Device Requirements	EDR 2.4 – Mobile Code	yes	7.10.2
	EDR 3.2 – Protection from malicious code	yes	7.10.3
	EDR 3.10 – Support for Updates	yes	7.10.4

Category	Requirement	Relevant	Details
	EDR 3.14 – Integrity of the boot process	yes	7.10.5
Host device requirements	HDR 2.4 – Mobile Code	no	7.11.2
	HDR 3.2 – Protection from malicious code	no	7.11.3
	HDR 3.10 – Support for Updates	no	7.11.4
	HDR 3.14 – Integrity of the boot process	no	7.11.5
Network device requirements	NDR 1.6 – Wireless access management	no	7.12.2
	NDR 1.13 – Access via untrusted networks	no	7.12.3
	NDR 2.4 – Mobile Code	no	7.12.4
	NDR 3.2 – Protection from malicious code	no	7.12.5
	NDR 3.10 – Support for Updates	no	7.12.6
	NDR 3.14 – Integrity of the boot process	no	7.12.7
	NDR 5.2 – Zone boundary protection	no	7.12.8
	NDR 5.3 – General purpose, person-to-person communication restrictions	no	7.12.9

7.2 FR 1 – Identification and authentication control

7.2.1 General

Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets.

7.2.2 CR 1.1 – Human user identification and authentication

Applicable to IO-Link

No

Justification

Not relevant because human users are not supposed to directly interact with the Device. The IO-Link protocol is a machine-to-machine protocol.

Comments

If a device has an additional interface suitable for human user interaction or a user interface (e.g., buttons, display), then the manufacturer needs to provide human user identification and authentication.

7.2.3 CR 1.3 – Account Management

Applicable to IO-Link

No

Justification

Each Device is always connected directly via a point-to-point connection to one Master and the Master always has the same level of access. Therefore, Masters do not identify or authenticate to Devices and Devices do not support account management (neither accounts for different Masters nor for different users).

Comments

IO-Link does support the concept of user roles in the sense that it is possible to specify different access permissions for different roles in IODD (IO-Link Device Description)

files. However, these roles, permissions and user accounts are supposed to be handled and enforced by the PDCT, not by the Device.

7.2.4 CR 1.4 – Identifier Management

Applicable to IO-Link

No

Justification

See 7.2.3

7.2.5 CR 1.5 – Authenticator Management

Applicable to IO-Link

No

Justification

See 7.2.3

7.2.6 CR 1.7 – Strength of password-based authentication

Applicable to IO-Link

No

Justification

See 7.2.3

7.2.7 CR 1.10 – Authenticator Feedback

Applicable to IO-Link

No

Justification

See 7.2.3

7.2.8 CR 1.11 – Unsuccessful Login Attempts

Applicable to IO-Link

No

Justification

See 7.2.3

7.2.9 CR 1.12 – System Use Notifications

Applicable to IO-Link

No

Justification

See 7.2.3

7.3 FR 2 – Use Control

7.3.1 General

Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.

7.3.2 CR 2.1 – Authorization Enforcement

Applicable to IO-Link

No

Justification

See 7.2.3

7.3.3 CR 2.2 – Wireless use control

Applicable to IO-Link

No

Justification

The assumed scenario does not include wireless communication.

7.3.4 CR 2.5 – Session lock

Applicable to IO-Link

No

Justification

See 7.2.2and 7.2.3

7.3.5 CR 2.8 – Auditable Events

Applicable to IO-Link

Yes

Contextual mapping

The Device shall use events to report security-related events to the Master. It shall use EventQualifier and EventCode as defined in the IO-Link standard to specify the type and ID of the event.

Events do not contain a field for timestamps. Therefore, when the Master or a following entity receives an event from a Device, then this entity shall create and store a timestamp with the received event.

7.3.6 CR 2.9 – Audit storage capacity

Applicable to IO-Link

Yes

Contextual mapping

Since Devices typically do not have synchronized clocks, Devices shall send events to the Master as soon as possible (see 7.3.5). Devices must provide sufficient storage capacity to store events until they have been transmitted to the Master and the Master has acknowledged the receipt of the event.

An IO-Link Device is not capable of reporting security events before communication is established. During this time, these security events will not be saved in the Device, as the IO-Link specification does not support persistence of events prior to established communication.

7.3.7 CR 2.10 – Response to Audit Processing Failures

Applicable to IO-Link

Yes

Contextual mapping

Devices shall ensure that audit processing failures do not impact essential services and functions. If audit storage capacity for events that have not yet been transmitted to the master is exceeded, then devices shall react appropriately, for example by overwriting the oldest event.

7.3.8 CR 2.11 – Timestamps

Applicable to IO-Link

No

Justification

Devices shall use events to report security-related events to the Master. The Master or a following entity shall create and store a timestamp with the received event. Therefore, Devices do not have to create timestamps.

7.3.9 CR 2.12 – Non-repudiation

Applicable to IO-Link

No

Justification

The Device does not provide a human user interface.

7.4 FR 3 – System Integrity

7.4.1 General

Ensure the integrity of the component to protect against unauthorized manipulation or modification.

7.4.2 CR 3.1 – Communication Integrity

Applicable to IO-Link

Yes

Comments

Currently, the IO-Link protocol does not offer protection against intentional modification (i.e., it does not make use of signatures or message authentication codes). However, IEC 62443-4-2, section 7.3.2, paragraph 2 states that physical access protection may be sufficient on lower SL-Cs. The scenario under consideration relates to wired point-to-point communication and security level SL-C 1, therefore physical access protection can be considered sufficient.

The integrator must decide whether and which level of physical protection of the IO-Link cable and Device is necessary.

Contextual mapping

Protection against unintentional modifications: The CRC specified in the IO-Link protocol will detect unintentional modifications.

Protection against intentional modifications: The IO-Link protocol does not offer integrity protection against intentional modifications. Therefore, the manufacturer should include the following (or a similar) paragraph in the user documentation: "It is recommended to perform a security assessment and to decide whether it is necessary to physically protect the IO-Link communication against intentional modification."

7.4.3 CR 3.3 – Security functionality verification

Applicable to IO-Link

Yes

Contextual mapping

The manufacturer should provide guidance in the user documentation on how to test the designed security controls of the Device, e.g.

– how can the user verify that the Device does not process messages with incorrect CRC
– how can the user verify that the Device rejects firmware updates that are not suitable for the Device
– how can the user verify that the Device reports events to the Master for specific security-relevant events

7.4.4 CR 3.4 – Software and information integrity

Applicable to IO-Link

Yes

Comments

The integrity of IODD files and IOLFW files can be verified via the CRC (protection against unintentional data corruption) in the IODD file, and optionally via digital signatures (protection against malicious actors, not standardized). Applications that process these files shall verify the CRC before utilizing the file to ensure its integrity.

Contextual mapping

The Device shall be able perform integrity checks on software and configuration data, for example by using digital signatures, cryptographic hashes or checksums, and to report integrity errors to the master via events or utilize external indicators to signal integrity issues, if available. The allowed Wake-up readiness following power-on (T_{RDL}) shall be considered.

Possible examples how to react to integrity checks: The device may decide to abort the boot process in case of integrity violations, or Devices may choose to simply provide integrity information to the master.

It is recommended to follow the recommendations of BLOB-Transfer&FW-Update V1.2.

The Device must provide a checksum over all user-changeable, non-volatile parameters to detect modifications to the parameterization within the application context.

7.4.5 CR 3.5 – Input Validation

Applicable to IO-Link

Yes

Contextual mapping

The Device shall validate the syntax, length and content of any input data. This includes all parts of received IO-Link messages including application data.

7.4.6 CR 3.6 – Deterministic Output

Applicable to IO-Link

Yes

Comments

This requirement does only apply to actuators.

Contextual mapping

If normal operation cannot be maintained (e.g., due to communication loss or other errors), actuator Devices shall set outputs to a predetermined state, e.g., set the output to a predefined fixed value, hold the last good value or go to an "unpowered" state.

The IO-Link protocol provides the information whether the communication state leaves the "normal operation". The application layer must react to this accordingly. [See IO-Link specification chapter 10.8.3 "Communication loss"]

7.4.7 CR 3.7 – Error Handling

Applicable to IO-Link

Yes

Comments

Elaborated error handling isn't defined as part of the protocol, therefore this requirement can only be violated by vendor specific implementations.

Contextual mapping

The Device shall identify and handle errors without revealing information that could be exploited by an attacker. Error messages shall, for example, not contain passwords, keys or detailed stack traces.

7.5 FR 4 – Data Confidentiality

7.5.1 General

Ensure the confidentiality of information on communication channels and in data stored in repositories to protect against unauthorized disclosure.

7.5.2 CR 4.1 – Information Confidentiality

Applicable to IO-Link

Yes

Comments

The IO-Link protocol currently does not support neither encryption nor user authentication.

Contextual mapping

- Requirement a), confidentiality of information at rest:
- IO-Link Devices typically do not contain confidential data for which read authorization would be required (since the IO-Link protocol does not support authentication), and therefore no action is required. IO-Link Devices that process or store confidential data (e.g., a firmware decryption key) shall implement access control mechanisms or encryption to protect confidential data at rest.
- Requirement b), protection of the confidentiality of information in transit:
- Since the IO-Link protocol does not support encryption, users shall protect the confidentiality of information in transit by restricting physical access to the IO-Link device and cable, if the data in transit requires confidentiality protection. The manufacturer shall describe this in the user documentation.

7.5.3 CR 4.3 – Use of cryptography

Applicable to IO-Link

Yes

Contextual mapping

No action is required for IO-Link Devices that do not use cryptography.

IO-Link Devices that use cryptography, for example for decrypting firmware or for verifying signatures of firmware files, shall follow recommended best practices regarding the used algorithms and key sizes.

7.6 FR 5 – Restricted Data Flow

7.6.1 General

Segment the control system via zones and conduits to limit the unnecessary flow of data.

7.6.2 CR 5.1 – Support Network Segmentation

Applicable to IO-Link

Yes

Comments

IO-Link is a point-to-point protocol, therefore it intrinsically supports the concept of network segmentation.

7.7 FR 6 – Timely response to events

7.7.1 General

Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

7.7.2 CR 6.1 – Audit log accessibility

Applicable to IO-Link

No

Justification

IO-Link Devices immediately report security-relevant events to the IO-Link Master (see 7.3.5). IO-Link Devices do not store events persistently. The IO-Link Master is responsible to store these events in its audit log and to provide access to it.

7.8 FR 7 – Resource Availability

7.8.1 General

Ensure the availability of components against the degradation or denial of essential services.

7.8.2 CR 7.1 – Denial of Service Protection

Applicable to IO-Link

No

Justification

IO-Link is a point-to-point protocol. Therefore, the IO-Link Device communicates with only one other device, either with a benign, standard-compliant Master or with a malicious or not-standard-compliant device.

In the former case, the IO-Link device must be able to process messages at the maximum possible rate for the supported transmission rate and handle errors properly.

In the latter case, the IO-Link Device cannot protect against DoS attempts by the other device because the other device can simply stop communicating with the IO-Link Device.

7.8.3 CR 7.2 – Resource Management

Applicable to IO-Link

No

Justification

The IO-Link device must be able to process messages at the maximum possible rate for the supported transmission rate.

Besides this, no action is required.

7.8.4 CR 7.3 – Control System Backup

Applicable to IO-Link

Yes

Contextual mapping

IO-Link devices shall support backup and restore of device data as specified in the IO-Link standard.

7.8.5 CR 7.4 – Control system recovery and reconstitution

Applicable to IO-Link

Yes

Contextual mapping

See 7.8.4

7.8.6 CR 7.6 – Network and security configuration settings

Applicable to IO-Link

Yes

Comments

IO-Link Devices do not have network settings.

Contextual mapping

If an IO-Link Device has configurable security settings, then it shall support configuration of these security settings, e.g. via configurable parameters.

7.8.7 CR 7.7 – Least Functionality

Applicable to IO-Link

Yes

Comments

Example: The IO-Link device has a local user interface (display and buttons) as an additional means to change configuration parameters.

Contextual mapping

If an IO-Link Device offers functions or services that are not necessary for basic IACS functionality then the device shall support disabling these non-essential functions and services, e.g. via configurable parameters.

7.9 Software Application Requirements

7.9.1 General

The purpose of this set of requirements is to document requirements that are specific to software applications.

7.9.2 SAR 2.4 – Mobile Code

Applicable to IO-Link

No

Justification

The IO-Link standard does not support mobile code in Devices.

7.9.3 SAR 3.2 – Protection from malicious code

Applicable to IO-Link

No

Justification

The IO-Link standard does not support mobile code in Devices.

7.10 Embedded Device Requirements

7.10.1 General

The purpose of this set of requirements is to document requirements that are specific to embedded devices.

7.10.2 EDR 2.4 – Mobile Code

Applicable to IO-Link

Yes

Comments

IO-Link Devices typically do not utilize mobile code technologies.

Contextual mapping

If an IO-Link Device utilizes mobile code technologies, then it shall provide the capability to enforce a security policy for the usage of mobile code technologies.

7.10.3 EDR 3.2 – Protection from malicious code

Applicable to IO-Link

Yes

Contextual mapping

The IO-Link Device shall verify the authenticity of a firmware update (e.g., via digital signatures) before installing the firmware update.

7.10.4 EDR 3.10 – Support for Updates

Applicable to IO-Link

Yes

Comments

The IO-Link Device shall support the ability to be updated and upgraded.

Possible options are firmware update via the IO-Link profile BLOB Transfer & Firmware Update or other manufacturer-specific update methods like device replacement.

Contextual mapping

The IO-Link Device manufacturer must ensure the possibility to update and/or upgrade devices.

7.10.5 EDR 3.14 – Integrity of the boot process

Applicable to IO-Link

Yes

Comments

SL-C 1 does not require to verify the authenticity (e.g., signature) of the firmware.

Keep in mind the maximum boot time for IO-Link Devices.

Configuration data includes both the factory configuration data and user-accessible configuration data.

Contextual mapping

The IO-Link Device shall verify the integrity of the firmware, software, and configuration data needed for the component's boot and runtime processes prior to use.

7.11 Host device requirements

7.11.1 General

The purpose of this set of requirements is to document requirements that are specific to host devices.

7.11.2 HDR 2.4 – Mobile Code

Applicable to IO-Link

No

Justification

Not a network device.

7.11.3 HDR 3.2 – Protection from malicious code

Applicable to IO-Link

No

Justification

Not a network device.

7.11.4 HDR 3.10 – Support for Updates

Applicable to IO-Link

582 No

583 **Justification**

584 Not a network device.

585

586 ### 7.11.5 HDR 3.14 – Integrity of the boot process

587 **Applicable to IO-Link**

588 No

589 **Justification**

590 Not a network device.

591

592 ## 7.12 Network device requirements

593 ### 7.12.1 General

594 The purpose of this set of requirements is to document requirements that are specific to network
595 devices.

596 ### 7.12.2 NDR 1.6 – Wireless access management

597 **Applicable to IO-Link**

598 No

599 **Justification**

600 Not a network device.

601

602 ### 7.12.3 NDR 1.13 – Access via untrusted networks

603 **Applicable to IO-Link**

604 No

605 **Justification**

606 Not a network device.

607

608 ### 7.12.4 NDR 2.4 – Mobile Code

609 **Applicable to IO-Link**

610 No

611 **Justification**

612 Not a network device.

613

614 ### 7.12.5 NDR 3.2 – Protection from malicious code

615 **Applicable to IO-Link**

616 No

Justification

Not a network device.

7.12.6 NDR 3.10 – Support for Updates

Applicable to IO-Link

No

Justification

Not a network device.

7.12.7 NDR 3.14 – Integrity of the boot process

Applicable to IO-Link

No

Justification

Not a network device.

7.12.8 NDR 5.2 – Zone boundary protection

Applicable to IO-Link

No

Justification

Not a network device.

7.12.9 NDR 5.3 – General purpose, person-to-person communication restrictions

Applicable to IO-Link

No

Justification

Not a network device.

Annex A
(informative)

Applicable laws

A.1 General

Here is a list of selected relevant laws that might impact security requirements for the development of devices. Note that the list is not exhaustive – thus consider specific laws based on the intended usage region of devices.

A.2 EU CRA

The Cyber Resilience Act (CRA) aims to enhance cybersecurity across the European Union by establishing common standards for products with digital elements. The key goals of the CRA include:

– Improving Security: Ensuring that all digital products, including hardware and software, meet high cybersecurity standards throughout their lifecycle.
– Manufacturer Responsibility: Shifting the responsibility for cybersecurity to manufacturers, requiring them to provide regular security updates and address vulnerabilities promptly.
– Consumer Protection: Safeguarding consumers by providing clear and comprehensive information about the cybersecurity features of.
– Reducing Cyber Risks: Mitigating the risks associated with cyberattacks, which can disrupt economic and social activities.

The CRA applies to a wide range of products with digital elements, including:

– Smart Home Devices: Thermostats, alarm systems, and cameras that have any type of communication interface.
– Wearables and Consumer Electronics: Smartwatches, fitness trackers, and other personal gadgets.
– Industrial IoT Components: Devices used in industrial settings that have communication capabilities.
– Communication Modules: Found in machinery, vehicles, and medical devices, facilitating communication.
– Gateways and Routers: Devices that manage network traffic and provide connectivity.

Obligations of manufacturers (simplified summary):

– Assess security risks for products and document the results.
– Apply security measures that are appropriate to the identified risks during planning, design, implementation, production, delivery and maintenance of the products.
– Ensure products do not contain exploitable security vulnerabilities (in own code and in included third party components).
– Provide a secure default configuration.
– Define and communicate an appropriate support period for each product (at least five years).
– Test and review the security of products.
– Ensure ways of addressing vulnerabilities, where possible and applicable through security updates and/or device upgrades.
– Handle vulnerabilities and provide indications on how to handle the possible need for updates and/or device upgrades, and provide security advisories during the support period.
– Implement mechanisms to prevent unauthorized access.
– Protect the confidentiality and integrity of data (stored, transmitted, or processed) via encryption and other technical measures.

690 – Adhere to data minimization principles by processing only necessary and relevant data.
691 – Maintain availability of essential functions after incidents through resilience and mitigation
692 measures.
693 – Minimize any negative impact on other devices or networks.
694 – Limit the product's attack surface and reduce incident impact through secure design.
695 – Record security-relevant activities in the log data.
696 – Allow users to securely remove data and settings, ensuring secure data transfer if neces-
697 sary.
698 – Provide security information in user documentation.
699 – Write (internal) technical documentation and keep it up to date: risk assessment, applied
700 security measures, design, development and production documentation, SBOM, vulnerabil-
701 ity handling and disclosure process, etc.
702 – Report actively exploited vulnerabilities to the designated computer security incident re-
703 sponse team and to ENISA.
704 These measures aim to create a safer digital environment for both consumers and businesses
705 within the EU.
706 Sources:

707 1) https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
708 2) https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
709 3) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402847

710

A.3 US executive order on cybersecurity

Essence of the 2025 U.S. Cybersecurity Executive Order

Purpose: Strengthen national cybersecurity and promote innovation in digital defense.

Scope: Applies to federal agencies and influences private sector practices through procurement and standards.

Key Focus Areas

– Secure Software Supply Chains: Enforce secure development practices and require verifiable security artifacts (e.g., SBOMs).
– Cloud Security Oversight: Increase accountability for cloud service providers handling federal data.
– AI in Cybersecurity: Promote secure AI development and use AI for cyber threat detection and response.
– Post-Quantum Cryptography: Accelerate adoption of quantum-resistant encryption standards.
– Digital Identity Verification: Support secure, remote identity verification using digital credentials.
– Rules-as-Code Pilot: Launch machine-readable cybersecurity policy initiatives to automate compliance.

Bibliography

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

[2] IO-Link Community, *IO-Link Interface and System Specification, Order No 10.002*

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

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

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

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

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

[8] IO-Link Community, IO-Link *Secure Deployment Guideline, Order No 10.502*

_____

IO-Link Community
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
http://www.io-link.com/