SICK Cybersecurity requirements for suppliers

Preface

It is a key objective of SICK to provide its customers with high-quality products and services. To achieve this goal, certain processes for continuous risk management regarding Cybersecurity of SICK products must be implemented. In addition, legal requirements (including the EU Cyber Resilience Act) oblige SICK, together with its suppliers, to ensure adequate Cybersecurity throughout the entire lifecycle of the products.

This document defines Cybersecurity requirements that must be met by suppliers for all products with digital elements (PDE) used in or as part of a SICK solution. In addition, preferred implementations are specified for some of the requirements.

The following requirements must be covered by the supplier (see Chapter 4):

- Responsibility for cybersecurity
- Security development process
- Supplier management for cybersecurity
- Transparency and response to cybersecurity
- Cybersecurity training
- Security of manufacturing

The “SICK Cybersecurity Supplier Requirements for Products” include requirements for the following types of suppliers:

- Component manufacturers
- Private-label manufacturers
- Manufacturing service providers

The respective requirements indicate for which type of supplier they are applicable. If “All suppliers” is specified, the requirement applies to component manufacturers, private-label manufacturers, and manufacturing service providers.

Definitions

Produkts with digital elements

Products with digital elements (PDE) are defined as described in the EU Cyber Resilience Act[1].

Right to Audit

SICK reserves the right, at any time (but no more than once every twelve months), to request additional documentation and evidence, as well as to conduct or commission a compliance audit in order to verify whether the specified requirements are met. Each party shall bear its own costs incurred in connection with the audit. The supplier is not obligated to bear the costs of the auditing party or any third parties commissioned by it. If gaps in the fulfillment of SICK's requirements are identified based on the supplier documentation or the audit results, the supplier shall, at its own expense, take all necessary measures and comply with all reasonable instructions from SICK in order to close the identified gaps without delay.

Requirements

Responsibility for Cybersecurity (Ownership for Cybersecurity)

OFC-01

- Applicable to: All suppliers
- **Requirement**: The supplier must systematically implement cybersecurity in accordance with organizational, legal, and market requirements. The supplier's management shall confirm cybersecurity as one of the key quality characteristics of the supplied products.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:52022PC0454

- **Preferred solution**: The supplier establishes a Cybersecurity Management System (CSMS) based on IEC 62443.

Cybersecurity in the Development Process (Security Development Process)

SDP-01

- Applicable to: All suppliers
- **Requirement**: The supplier must develop the supplied product using an established cybersecurity development process in line with the industry state of the art.
- **Preferred solution**: The supplier's cybersecurity development process is certified (e.g., according to IEC 62443-4-1).

SDP-02

- Applicable to: All suppliers
- **Requirement**: The supplier's cybersecurity development process must include a risk-based approach to cybersecurity measures. Identified residual risks and all relevant assumptions must be documented and provided with the supplied product.
- **Preferred solution**: The implemented risk analysis is standardized across the supplier's entire development organization. Identified remaining risks must be documented as part of the offer.

SDP-03

- Applicable to: Component suppliers

- **Requirement**: The supplier must document a Software Bill of Materials (SBOM) with the direct dependencies for the supplied product. In the event that SICK is required to provide the SBOM for a SICK PDE that integrates the supplied product to competent authorities, the supplier must provide the SBOM for the supplied product.

- **Preferred solution**: The SBOM is available in "CycloneDX" format or alternatively in another widely used machine-readable format (e.g., SPDX). The SBOM includes subcomponents (transitive dependencies). Entries in the SBOM for commercial software components include a contact option for the component. The SBOM is part of the delivery or is made available via an endpoint from which SICK can download it.

SDP-04

- Applicable to: Private-label suppliers

- **Requirement**: The supplier must provide an SBOM for the supplied product that includes direct dependencies.

- **Preferred solution**: The SBOM is available in "CycloneDX" format[2] or alternatively in another widely used machine-readable format (e.g., SPDX). The bill of materials includes subcomponents (transitive dependencies). Entries in the bill of materials for commercial software components include a contact option for the component. The SBOM is part of the delivery or is made available via an endpoint from which SICK can download it.

SDP-05

- Applicable to: Private-label suppliers, component suppliers

- **Requirement**: The supplier must deliver the supplied product without known exploitable vulnerabilities. The supplier must use appropriate means to

[2] https://cyclonedx.org/docs/1.6/json/

search for exploitable vulnerabilities.

- **Preferred solution**: The supplier uses methods such as static code analysis, security testing, and continuous checks against publicly known vulnerabilities during the development of the supplied product.

Supplier Management for Cybersecurity (Supplier Management for Cybersecurity)

SMC-01

- Applicable to: Private-label suppliers, component suppliers
- **Requirement**: The supplier requires and ensures that its own suppliers take cybersecurity into account based on established industry standards.

Transparency and Reaction Requirements (Transparency and Reaction Requirements)

TRR-01

- Applicable to: All suppliers
- **Requirement**: The supplier must establish a dedicated contact option accessible to SICK for reporting vulnerabilities.
- **Preferred solution**: The contact is specified in a security.txt file in accordance with RFC 9116[3].

TRR-02

- Applicable to: All suppliers

[3] https://www.rfc-editor.org/rfc/rfc911

- **Requirement**: The supplier must inform SICK of cybersecurity incidents within its organization that may affect the security of the supplied PDEs without delay and, upon request by SICK, cooperate closely with SICK to remediate vulnerabilities.

- **Preferred solution**: The supplier notifies SICK within 24 hours of discovering the vulnerabilities via email to psirt@sick.de (using PGP encryption).

TRR-03

- Applicable to: Private-label suppliers, component suppliers

- **Requirement**: The supplier must establish an incident response process, provide appropriate resources, and ensure the effectiveness of the process. The incident response process must include a vulnerability disclosure mechanism accessible to SICK. The supplier must respond appropriately and without delay to vulnerabilities and cybersecurity incidents related to all supplied PDEs.

- **Preferred solution**: A coordinated vulnerability disclosure process is established. The supplier supports vulnerability notifications using the machine-readable CSAF format[^5]. For confidential information, notification to SICK via email to psirt@sick.de using PGP encryption is preferred.

TRR-04

- Applicable to: Private-label suppliers, component suppliers

- **Requirement**: If exploitable security vulnerabilities in the supplied product become known to the supplier, the supplier must provide security updates for the supplied product without delay, typically within 30 days.

- **Preferred solution**: Notification of the update is communicated using the machine-readable CSAF format. For confidential information, it is preferred to inform SICK via email to psirt@sick.de using PGP encryption.

Cybersecurity Education (Cybersecurity Education)

CED-01

- Applicable to: Private-label suppliers, component suppliers
- **Requirement**: The supplier must provide a cybersecurity training program that is available to personnel contributing to product development and whose participation can be demonstrably verified.

Supply Chain and Production Security (Supplychain and Production Security)

PRD-01

- Applicable to: All suppliers
- **Requirement**: The supplier must adequately protect the production areas of the supplied product against physical access by persons (e.g., third parties or employees) who are not authorized by the supplier.
- **Preferred solution**: The physical protection has been tested through physical penetration tests.

PRD-02

- Applicable to: All suppliers
- **Requirement**: The supplier must protect the production areas of the supplied product against digital access (e.g., network access) by persons (e.g., third parties or employees) who are not authorized by the supplier.
- **Preferred solution**: Solutions for network segregation are in place. Networks are monitored. Digital protection has been tested through penetration tests. Relevant processes, IT assets, and production networks are certified according to ISO 27001, IEC 62443, or other established IT security standards.

PRD-03

- Applicable to: All suppliers
- **Requirement**: The supplier must adequately protect the manufacturing, storage, and delivery of the supplied product against cyber threats.
- **Preferred solution**: Relevant processes, IT assets, and production networks are certified according to ISO 27001, IEC 62443, or other established IT security standards.

PRD-04

- Applicable to: All suppliers
- **Requirement**: If digital data is exchanged between the supplier and SICK for the purpose of development, production, manufacturing, or delivery of the supplied product, the sender must use a secure transmission method.
- **Preferred solution**: Data exchange uses solutions provided by SICK (e.g., https://ftp.sick.com).

Signed in confirmation of the requirements

Place, Date

Signature

Name

Position

Company