Swegon

Sensitivity	Public
Owner	Head of Cybersecurity
Date	2026-11-17

Swegon Security Requirements for OT/ICS

Information Security

2026-11-17 | Version 1.2



Table of Contents

1. Introduction 2
1.1. Purpose 2
1.2. Scope 2
2. Guidance 3
3. OT/ICS Requirements 4
3.1. Solution Governance 4
3.2. Regulatory Compliance 4
3.3. System Classification 4
3.4. Secure Development 5
3.5. Network Documentation 5
3.6. Network Segmentation and Access Control 5
3.7. Vendor Remote Access 5
3.8. Authentication and Accounts 5
3.9. Operating Systems and Lifecycle 6
3.10. Configuration and Hardening 6
3.11. Instructions and Documentation 6
3.12. Security Validation 6
3.13. Removable Media 6
3.14. Wireless Communications 6
3.15. Engineering Workstations 6
3.16. Insecure Protocols 7
3.17. Patch and Vulnerability Management 7
3.18. Logging and Monitoring 7
3.19. Cryptography 7
3.20. Backup and Configuration Recovery 7
3.21. Physical Protection 7
3.22. Change Management 8
3.23. Incident Response 8
3.24. Decommissioning 8
4. Exceptions 9
5. Related Resources 10
6. References 11
7. Document History 12

1. Introduction

1.1. Purpose

Swegon is committed to ensuring the availability, confidentiality, integrity and accountability of data, systems, and services. This document establishes minimum security requirements for the procurement, integration, operation, and decommissioning of operational technology and industrial control systems (OT/ICS) at Swegon-operated facilities.

The requirements are aligned with ISA/IEC 62443 and informed by NIST SP 800-82. It supplements Swegon Security Requirements for IT Service Providers and is a sibling to Swegon Security Requirements for IT Solutions, focused on the distinct security model of OT/ICS environments.

1.2. Scope

The requirements outlined in this document apply to any OT/ICS system delivered to and operated at Swegon production sites, whether procured from external suppliers or implemented by internal Swegon teams, including:

- **Production OT**: programmable logic controllers (PLCs), human-machine interfaces (HMIs), supervisory control systems, engineering workstations, and machinery-control PCs.
- **Facility OT**: building automation systems, CCTV, electronic access control, and other facility services on isolated network segments.

This document covers OT/ICS systems that Swegon operates at its own facilities. Swegon products with digital elements that Swegon places on the market are governed by Swegon Security Requirements for Products with Digital Elements and product-specific requirements documents.

A system in operation before this document is brought under it through Retrospective Governance in the Swegon Asset Management Guidelines, prioritised by risk; where a requirement is not feasible for legacy equipment, the rationale and compensating controls are documented as described in section 4.

2. Guidance

OT/ICS systems differ materially from general IT in lifecycle (often 15-20+ years), patch availability, vendor support models, and the consequence of disruption. Where this document refers to industry frameworks, suppliers should consult ISA/IEC 62443 (especially -2-1 for asset owner programmes, -3-3 for system requirements and Security Levels, and -4-1/4-2 for component vendors) and NIST SP 800-82 for additional guidance.

> **Note**: Security controls shall not compromise the functional safety of OT/ICS systems. Where a security control would interfere with emergency response, safety functions, or certified safety instrumented systems (SIS), the control shall be adapted, deferred, or replaced with a compensating measure agreed with Swegon.

3. OT/ICS Requirements

The supplier shall comply with these requirements as a minimum in a manner proportionate to the criticality of the system, supplemented by Swegon Security Requirements for IT Service Providers and any project- or system-specific additional requirements. The requirements apply equally to subcontractors and third-party providers used by the supplier in the delivery, and equivalently to internal Swegon teams where they take the role of supplier in delivering an OT/ICS system.

Exceptions to these requirements are handled as described in section 4.

3.1. Solution Governance

Delivered OT/ICS systems shall be onboarded through Swegon's IT Solution Governance Process. The supplier shall provide the information needed for onboarding (system identification, architecture, ports and services with justification, accounts, support contract details).

3.2. Regulatory Compliance

Delivered systems shall support Swegon's compliance obligations under the EU NIS2 Directive and Swedish Cybersäkerhetslagen. Systems processing personal data, in particular CCTV and electronic access control, shall support Swegon's compliance with the General Data Protection Regulation (GDPR).

Where a delivered OT/ICS system is itself a product subject to EU product cybersecurity legislation (e.g., the Cyber Resilience Act, or the Radio Equipment Directive where it incorporates a radio interface), the supplier is responsible for product-level conformity, including the technical file, declaration of conformity, CE marking, and ENISA vulnerability notifications.

For every delivered system, as the operating environment, Swegon requires that the supplier:

- Commit to a security support period of at least five (5) years from delivery, set with regard to the time the system is expected to be in use.
- High-classification OT typically has an asset life of 15-20 years; for those systems the support period is agreed at procurement and recorded in the support contract.
- Maintain capability to provide security updates and vulnerability patches during the support period.

3.3. System Classification

Swegon assigns each delivered system a risk classification (Low / Medium / High), determined by Swegon and communicated to the supplier at procurement. The supplier shall provide the information needed for the assessment.

The classification determines the target Security Level (SL-T) that Swegon assigns to the zones and conduits in which the system is placed. The supplier shall show that the delivered system is capable of meeting the IEC 62443-3-3 system requirements for that level (SL-C):

- SL 2 for High-classification systems, and
- SL 1 for Medium- and Low-classification systems.

3.4. Secure Development

Suppliers shall demonstrate alignment with ISA/IEC 62443-4-1 (secure product development lifecycle) for the supplied components, where applicable. Where the OT/ICS system includes custom software components such as custom applications, web or cloud-side components, or supplier-developed integrations, Swegon Security Requirements for IT Solutions applies additionally to those components.

3.5. Network Documentation

The supplier shall provide the system architecture, data flow, and protocol documentation that Swegon needs for its site network documentation (OT/ICS zones, conduits between zones, and boundaries with corporate IT networks), and shall update this documentation when changes are made.

3.6. Network Segmentation and Access Control

Delivered OT/ICS systems shall be deployed on Swegon-designated isolated network segments and shall not connect to Swegon's general-user network. The supplier shall design for outbound traffic from OT segments being denied by default, and shall provide a documented list of all destinations, protocols, and ports required for normal and emergency operation so that the necessary exceptions can be reviewed and authorised.

Communications between zones of different security levels shall pass through a documented conduit and shall originate from the higher-security zone where technically feasible. Direct connections between OT/ICS systems and external networks shall be permitted only through Swegon-provided network equipment and documented conduits.

Where Swegon operates Network Access Control (NAC) at OT network entry points, delivered systems should support NAC compatibility (e.g., 802.1X). Where NAC compatibility is not feasible for the system, the supplier shall disclose this at procurement and propose alternative network-level controls.

3.7. Vendor Remote Access

Vendor remote access to OT/ICS systems shall be initiated only via a Swegon service ticket and shall be time-bound, using Swegon-approved tools.

Suppliers shall not introduce alternative remote access channels (cellular modems, supplier-operated VPNs, or similar) without prior Swegon approval. Authentication for vendor remote access shall be distinct from authentication used inside the OT network. The supplier shall accept that sessions are logged and, where the tool supports it, recorded.

3.8. Authentication and Accounts

Delivered systems shall support individual user accounts, multi-factor authentication where the system permits, and credential transmission and storage in encrypted form. Default, guest, and vendor-owned accounts shall be disabled, removed, or transferred to Swegon at handover (when Swegon accepts operational responsibility for the system). Where the system requires shared accounts, the supplier shall disclose this at procurement so Swegon can record the exception.

3.9. Operating Systems and Lifecycle

Delivered OT/ICS systems shall run vendor-supported operating systems. Where the supplier delivers a system requiring an end-of-life or unsupported operating system, the supplier shall disclose this at procurement, identify the support status of the OS in use, and propose compensating controls (network isolation, application allowlisting, no internet or email access, removable-media restrictions). Such configurations require explicit Swegon approval and are recorded as documented exceptions.

3.10. Configuration and Hardening

Delivered OT/ICS systems shall be hardened by the supplier before delivery: secure defaults applied, default credentials changed, unused ports and services disabled, unnecessary software removed. The supplier shall provide a documented list of all ports, services, and accounts required for normal and emergency operation, with justification. Any hard-coded credentials, backdoor codes, or undocumented access paths shall be disclosed at procurement.

3.11. Instructions and Documentation

Delivered OT/ICS systems shall include documentation detailing secure configuration, operation, maintenance, and recovery procedures. Documentation shall be provided in a format Swegon can retain and shall be updated when material changes occur.

3.12. Security Validation

The supplier shall validate the security of delivered OT/ICS systems through testing appropriate to the system type (vulnerability scanning, penetration testing, fuzzing, conformance testing) before delivery. The supplier shall provide Swegon with a summary of the testing and its results. For High-classification systems, the testing should be carried out by a party independent of the supplier’s development team, or equivalent assurance shown, such as certification against IEC 62443, and the attestation shared with Swegon. Systems shall be delivered without known exploitable vulnerabilities. Vulnerabilities discovered after delivery shall be disclosed to Swegon, addressed, and remediated per the support agreement.

3.13. Removable Media

Removable media on OT/ICS systems shall be prohibited by default; where required for maintenance, media shall be Swegon-supplied and scanned before use. Delivered systems shall support physical port lockdown (USB blockers, sealed service ports) on ports not required for runtime operation.

3.14. Wireless Communications

Wireless communications (Wi-Fi, Bluetooth, cellular, LoRaWAN, proprietary radio) on delivered OT/ICS systems shall be disclosed at procurement. Unauthorised wireless capability shipped enabled by the supplier (e.g., Bluetooth on engineering workstations) shall be disabled before delivery. Authorised wireless paths shall use certificate-based authentication where the protocol supports it.

3.15. Engineering Workstations

Engineering workstations supplied to Swegon (those used to program PLCs, configure OT/ICS systems, or load controller firmware) shall be dedicated to OT use, with no general-

purpose computing functionality and no direct internet or corporate email access. They shall enforce multi-factor authentication where supported.

> **Note**: This section does not apply to operator consoles or HMIs that are themselves the production interface.

3.16. Insecure Protocols

Where OT/ICS systems use protocols without authentication or encryption (e.g., Modbus, Profinet without security, OPC Classic, Telnet, FTP), the supplier shall disclose this at procurement and shall use secure protocol variants (e.g., OPC UA over TLS, Modbus TCP over TLS, HTTPS for management interfaces) in preference where the system supports them.

3.17. Patch and Vulnerability Management

The supplier shall provide patches for the components they supply, qualify each patch against the deployed configuration, and notify Swegon of available security updates within a pre-negotiated window. The allocation of patch application between Swegon and the supplier, including scheduling of maintenance windows, application, and verification, shall be agreed at procurement and recorded in the support contract. Where IT-standard remediation timelines are not feasible, the supplier shall propose compensating controls per Swegon's Vulnerability Management Guidelines.

3.18. Logging and Monitoring

Delivered OT/ICS systems shall produce logs in accordance with Swegon's Logging and Monitoring Guidelines where the system technically supports it. Where the system cannot generate detailed logs (especially PLCs and embedded controllers), the supplier shall disclose this.

3.19. Cryptography

Delivered OT/ICS systems shall comply with Swegon's Cryptography and Key Management Guidelines where the system technically supports it. Software and firmware updates shall be cryptographically signed by the supplier and verified by the system before installation, where supported.

3.20. Backup and Configuration Recovery

The allocation of backup operations between Swegon and the supplier, including frequency, storage location, periodic restoration testing, and recovery time and recovery point objectives, shall be agreed at procurement and recorded in the support contract, aligned with Swegon's Business Continuity Guidelines.

3.21. Physical Protection

OT/ICS equipment shall be designed for installation within machine enclosures, locked cabinets, or otherwise physically restricted areas, not in unsecured spaces. Locking enclosures supplied by the vendor shall provide multiple identifiable keys per lock. Physical access to OT/ICS spaces is controlled per Swegon's Physical Security Guidelines.

3.22. Change Management

Changes to OT/ICS systems shall be coordinated through Swegon's change management process. Changes that affect machinery operation shall include a safety review. The supplier shall provide advance notice of major or high-risk changes, including patch releases, configuration changes, and firmware upgrades.

3.23. Incident Response

OT/ICS incidents follow Swegon's Incident Response Process. The supplier shall participate in containment and forensic activity as agreed in the support contract.

3.24. Decommissioning

At end of life, the supplier shall cooperate with Swegon's decommissioning process. Sensitive data, configurations, and credentials shall be securely removed from the system and from any supplier-held copies. Vendor-issued certificates and accounts shall be revoked.

4. Exceptions

Where a requirement is not fully applicable or feasible, which is common for legacy OT, the supplier shall document the rationale and propose compensating controls. An exception applies only once Swegon has confirmed it in writing. An agreed exception records the affected requirement, the rationale, the compensating controls and a review date.

Exceptions are time-limited where possible. An exception cannot override a legal or regulatory obligation.

5. Related Resources

The following resources are related to this document and may be consulted for further context. The Swegon guidelines and processes among them are internal documents; they are available on request.

- Swegon Information Security Policy
- Swegon Asset Management Guidelines
- Swegon Cryptography and Key Management Guidelines
- Swegon Logging and Monitoring Guidelines
- Swegon Vulnerability Management Guidelines
- Swegon Physical Security Guidelines
- Swegon Business Continuity Guidelines
- Swegon Incident Response Process
- Swegon Security Requirements for IT Solutions
- Swegon Security Requirements for IT Service Providers

6. References

This document is designed to support compliance with the following regulations, and is aligned with the following standards and frameworks:

Regulations

- EU General Data Protection Regulation (GDPR)
- EU NIS2 Directive
- EU Cyber Resilience Act (CRA)

Frameworks & Methodologies

- ISA/IEC 62443 series (Industrial communication networks - IT security for networks and systems)
- NIST SP 800-82 (Guide to Operational Technology Security)

7. Document History

VERSION	DATE	AUTHOR	DESCRIPTION
1.2	2026-11-17	Head of Cybersecurity	Scope extended to systems already in operation; the Radio Equipment Directive named for systems with a radio interface; support period of at least five years; security capability (SL-C) shown for the level Swegon assigns; test results shared with Swegon; exceptions in a section of their own.
1.1	2026-06-05	Head of Cybersecurity	Clarified inbound/outbound boundary with Products with Digital Elements; clarified that product-level CRA/RED conformity for delivered products sits with the supplier
1.0	2026-05-07	Head of Cybersecurity	Initial version