TECHDOCS

WAGO I/O System Field

Cybersecurity

765-xxx

Cybersecurity Manual
4446174731 | 3 | en-US | 2025-08-04 12:00

WAGO GmbH & Co. KG
Hansastraße 27
D - 32423 Minden
Phone: +49 571/887 – 0
Fax: +49 571/887 – 844169
E-Mail: ✉ **info@wago.com**
Internet: **www.wago.com**

Technical Support
Phone: +49 571/887 – 44555
Fax: +49 571/887 – 844555
E-Mail: ✉ **support@wago.com**

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: ✉ **documentation@wago.com**

Table of Contents

1 Scope of Applicability

This document applies to:

Products of WAGO I/O System Field (Series 765).

ⓘ Note

Note applicable documents!

The complete operating instructions for the product consists of several, applicable documents. The product must only be installed and operated in accordance with the complete operating instructions. Knowledge of all applicable documents is required for proper use. You can find all documents and information on the product detail page.

You can find all the documents and information at:

www.wago.com/all-765

You can access the product details page in the following ways:

- Scan the QR code printed on the product or instruction leaflet.
- Use the following address in your internet browser:
  www.wago.com/<item number>.
  Example: www.wago.com/765-1205/100-000 for item 765-1205/100-000.
- Visit the online catalog at: **www.wago.com**/and navigate to the item.

Applicable document

📖 **Product Manual** of the product used

2 Threats

2.1 Cybersecurity Threat in General

Probability and Severity of Events

Products for industrial automation can be used in a wide variety of systems and applications. Depending on the application, the requirements for the **protection goals** of cybersecurity (integrity, availability or confidentiality of data) can vary. The incentives for potential attackers and the severity of cybersecurity incidents are just as varied.

As the manufacturer, we can describe the circumstances under which unauthorized access can be gained to which data areas, interfaces or functions of our product. Targets can be considered from the **product perspective**. As a manufacturer, we can provide instructions on how to use the product's cybersecurity capabilities to reduce the likelihood of unauthorized access.

From an **application point of view**, the operator must check what damage can occur, what level of security is required and whether additional measures are needed to increase security. One criterion for the appropriateness of the level of security, for example, is whether or not personal data is processed in the specific application. Only the operator can assess the actual effects of unauthorized access in the respective specific application.

2.1.1 Targets from a Product Perspective

From a product perspective, at least the following physical or logical objects can represent targets of an attack:

- Disrupt product function (restrict availability).
- Manipulate data (influencing evaluations, decisions or system behavior).
- Making data accessible to unauthorized persons (third parties).
- Access to connected other systems.

2.1.2 Attack Vector from Product Perspective

From a product perspective, at least the following basic mechanisms can represent targets of an attack:

- Power supply interruption:
  Denial of Service (DoS) or planning of further attacks
- Access to unencrypted interfaces:
  Unauthorized operation of interfaces; multiple targets, potentially including the transmission of manipulated software/firmware
- Access to unencrypted data:
  Unauthorized use, disclosure or manipulation of data
- Changes to the structure, configuration or programming of the product:
  Multiple targets, potentially compromising other connected systems

2.2 Cybersecurity-Specific Threats

Specific threats can only be assessed with knowledge of the respective system and application. The operator must assess the threats arising from the significance of the data transmitted. Regardless of the assessment of transmitted data, basic types of threats to the specific product type can be identified.

Basic threat types specific to the product type: WAGO I/O System Field

- Interference with communication in the network:
  By manipulating the network address of the product, address conflicts can be created, communication interrupted or data misrouted.
- Acquisition of information about system processes:
  By recording the process input or process output data, information about processes running in the system can be obtained. This knowledge makes it possible to identify additional vulnerabilities for cybersecurity attacks.
- Disrupting processes or causing damage to the system:
  By manipulating process input data, the higher-level control system can be caused to generate incorrect setpoint values for decentralized automation devices. By manipulating process output data, field-level actuators can be caused to perform incorrect operations.

2.3 Vulnerability Assessment

Products have technical limits due to their product functions. These technical limits can represent a cybersecurity vulnerability.

If the operator compensates for these vulnerabilities with their own technical or organizational measures, the product can still be used safely.

The Cybersecurity Manual describes as targets which product features represent a known cybersecurity vulnerability if the operator does not take appropriate protective measures.

Note: The operator is responsible for evaluating all documented targets in terms of the probability of occurrence and severity of incidents and for taking appropriate measures. The vulnerability assessment must be extended to potential vulnerabilities that arise from the integration into the respective system and application.

The vulnerability assessment supports the achievement of the protection goals of data integrity, availability or confidentiality.

3 Vulnerabilities in Network Access

3.1 Vulnerabilities in Network Access – Overview

The product is intended for use in a protected network segment.

The following attacks are possible in an unprotected network segment through unauthorized access:

Data can be read out. Data can be manipulated. Data can be passed on to unauthorized persons (third parties).

The following data can be affected, for example:
- Product/device data, process data, configuration data, register data, parameterization data

Configurations can be read out. Configurations can be manipulated. Configurations can be passed on to unauthorized persons (third parties).

The following configurations may be affected:
- Product/device configurations, project configurations, network configurations

Software/firmware can be read out. Software/firmware can be manipulated. Software/firmware can be passed on to unauthorized persons (third parties).

The following software/firmware can be affected:
- Product software/firmware, service/auxiliary software

Systems can be read out. Systems can be manipulated. Systems can be compromised.

The following systems may be affected:
- I/O system, other connected systems

3.2 Insecure Fieldbus

The fieldbus connects higher-level wired controllers to the I/O system products and provides data exchange among the components.

An insecure fieldbus lacks cybersecurity capabilities like authentication, integrity protection and encryption.

Examples of insecure fieldbuses include PROFINET, EtherCAT and EtherNet/IP.

3.3 Unprotected Integrated Webserver

An integrated Webserver is used for product configuration. Websites on a Webserver can be accessed via the Internet or the network.

An unprotected integrated Webserver lacks cybersecurity capabilities like integrity protection and encryption.

3.4 Engineering/Service Access

Engineering/service access is used for configuration and parameterization.

The protocols do not support authentication or encryption.

Engineering/service access requires an engineering, configuration and parameterization tool running on an external engineering device (such as a desktop, laptop or smartphone).

An engineering device’s cybersecurity capabilities depend on many factors.

In particular, these include:
- The operating system
- The user rights
- If it connects to various different networks (e.g., publicly accessible networks)
- If it connects to portable data storage devices

If the engineering device is not sufficiently secure, the product data can be read out or manipulated via unauthorized users and/or malware.

4 Vulnerabilities in Physical Access

4.1 Physical Access Vulnerabilities – Overview

The product is intended for use in an area with physical access protection.

In areas without physical access protection, unauthorized access can permit the following attacks:

Connections can be interrupted or rendered inoperative, affecting product accessibility.

The following connections may be affected:
- Network connection

Data can be read out. Data can be manipulated. Data can be passed on to unauthorized persons (third parties).

The following data can be affected, for example:
- Product/device data, process data, configuration data, register data, parameterization data

The product can be reset to the factory settings, allowing access with the default username and password.

The following settings may be affected:
- Product/device settings

Components of the I/O system can be switched out. Components that have been manipulated can be inserted into the system.

The following components may be affected:
- Components of the I/O system

The software/firmware can be switched out. Software/firmware that has been manipulated can be introduced into the system.

The following software/firmware may be affected:
- Software/firmware of the I/O system components

4.2 Wireless Technology

Wireless technology makes it possible to configure devices and perform diagnostics without a physical connection.

Its range depends on the specific wireless technology used.

4.3 Network Interface

The network interface physically connects the product to the network. The network interface allows access to process data and product configurations.

5 Potential Targets

5.1 Non-Monitored Indicators

The product is intended for use in a secure operating environment.

The product is not capable of recognizing indications that a cyber attack is being prepared or carried out.

The product is not able to take sufficient countermeasures of its own when such incidents occur or operations are carried out. The lack of self-diagnostics gives attackers an opportunity to find and exploit vulnerabilities through experimentation.

Examples of indicators for planning or execution of cybersecurity attack are:
- Changed – usually increased – network activity
- Changed – usually increased – utilization of hardware
- Frequent successive changes to configurations

6 Hardening and Cybersecurity Capabilities

6.1 Defense-in-Depth Principle

The product is a device with open interfaces and ports and is intended for use in a protected network segment. Protective measures suitable for the specific application area and application must be implemented.

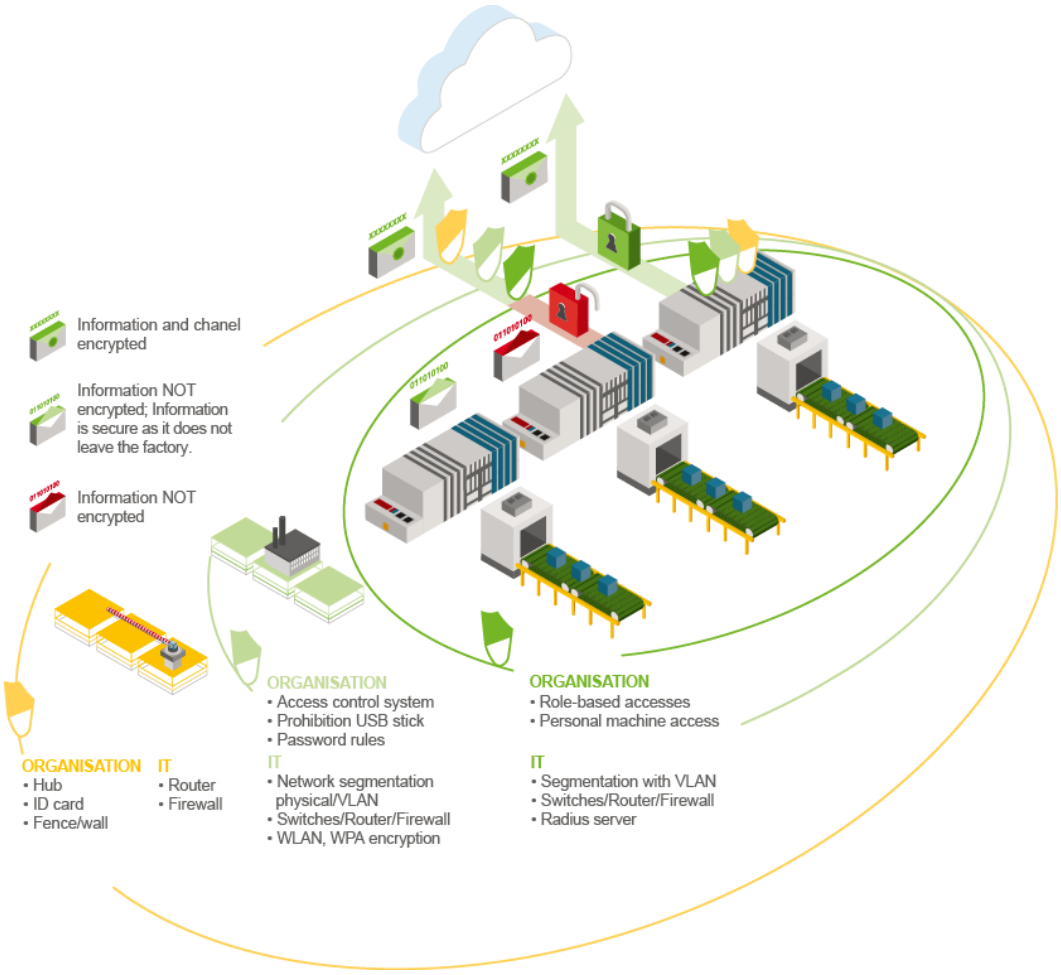

Figure 1: Onion Pattern (Example)

The system operator must combine organizational and technical security measures to successfully counter cybersecurity threats.

No single security measure offers comprehensive protection. For example, the hardness of a vault door (technical security measure) is irrelevant while the door for storage or retrieval is open (organizational security measure).

The function of some products requires that processes take place without protective measures (“safe door open”) within trust boundaries or within certain periods of time. Any protective functions missing from the product must then be implemented by the operator in the operational environment for which they are responsible.

The organizational and technical security measures taken must, like the layers of an onion, envelop all vulnerable access points or transmission paths and cover all areas that could be attacked. The security measures taken must also be designed in such a way that if one measure is overcome, the other measures continue to provide protection.

To aid in the interpretation of the security architecture, this documentation contains information on the necessary measures that can be identified from the product's point of view: **Hardening Measures [▶ 12]**.

6.2 Reference Architecture

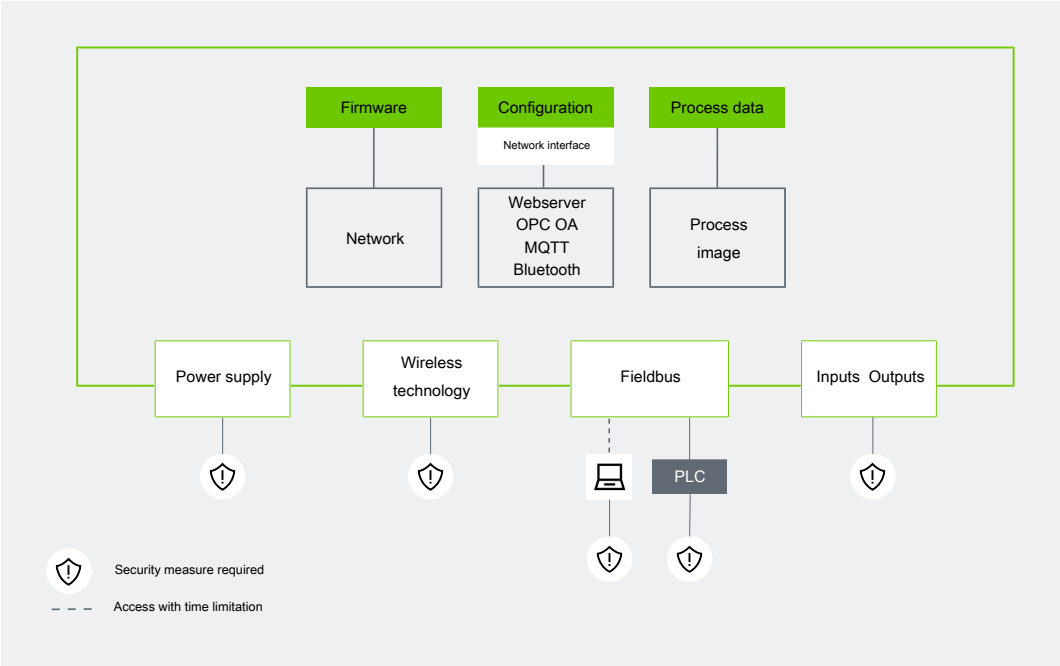

Figure 2: Reference Architecture

6.3 Hardening Measures

The hardening measures described are not alternatives to one another. To ensure good protection, the various hardening measures must be implemented in addition to each other.

6.3.1 Safe Operating Environment

The product must only be operated in a secure operating environment. A secure operating environment helps prevent various attacks. A secure operating environment meets the following requirements at a minimum:

- Physically protected access
- Protected network segment
- Recorded access and entry
- Monitoring for suspicious events or processes

Physically protected access

The product is a device with accessible connections.

It must only be installed in electrical operating rooms that meet the following requirements at a minimum:
- Access area is protected.
- Access is only granted to authorized persons.

Protected Network Segment

The product is a device with open interfaces and network ports. It may only be used in a protected network segment that meets the following requirements at a minimum:
- There is no unprotected connection to the Internet.
- There is no unprotected connection to other network segments.
- Access is authorized according to the reference architecture.
- All network devices are located in a protected network segment.

Recorded access and entry

In certain situations, the product requires temporarily reduced security. For example, temporarily reduced security may be necessary for engineering/service activities or in the event of a fault.

At a minimum, logging must capture the following events:
- Connecting an engineering device
- Access to the protected network segment (e.g., changing the limit of the protected network segment, disabling the firewall of the network)
- Access to the physically protected area (e.g., service personnel)

Monitoring for suspicious events or processes

Monitoring must cover at least the following events and processes:
- Changed, in particular suspiciously increased network activity

6.3.2 Secure Commissioning

Secure product commissioning helps prevent various attacks. Secure commissioning meets the following requirements at a minimum:
- Changed access data
- Protected network access

Access Data

- Change all freely accessible and documented access data.

The access data is freely accessible and documented in 🕮 **Product Manual**.

The following settings must be met at a minimum:
- Default passwords/login have been changed.
- Unused network ports are disabled.
- The network ports of used services are changed, provided that this can be reasonably implemented on the product itself and on the other side.
- Unused interfaces are disabled.
- Unused wireless technology is disabled.

Network Access

- Protect network access.

Die folgenden Anforderungen müssen mindestens erfüllt sein:
- Functions for network protection of the product are used if available (e.g., MAC filter).
- Secure protocol is used when available (e.g., HTTPS, SFTP).
- Only required interfaces are enabled.
- Only required network ports are enabled.
- Only necessary services are enabled.

6.3.3 Secure Operation

Secure operation of the product helps prevent various attacks. Secure operation meets the following requirements at a minimum:
- Time-limited physical access for engineering/service activities or in case of error
- Time-limited access and entry for engineering/service activities or in the event of a fault
- Security event/process logging
- Action following a security event/incident
- System integrity checks after changes
- Use of tested and current firmware/update
- Use of tools to check cybersecurity

Access and entry for engineering/service activities or in the event of a fault

Engineering or service activities often require access to product data or configuration. Therefore, the operator must ensure that the third-party devices used and the connection to the product are secure.

- Only grant access for a limited time.

The following forms of access must have time limitations:
- Access to communication software
- Access to interfaces
- Access with increased rights

Logging Security Incidents

- Log security events.

The following requirements for logging security events must be met as a minimum:
- The product's logging function is set up.
- Logging measures for security events that the product does not log have been set up.
- Logging measures for the network are set up.

WAGO recommends using “System Logging Protocol” (Syslog).

After a Security Incident

- Take action following a security event.

The following actions must be taken after a security event, as a minimum:
- Compare actual and setpoint configuration data.

System Integrity Checks

- Check the integrity of your system after any changes are made.

At a minimum, the following checks must be performed after configuration changes:
- Firewall check

Verified and current firmware (updates)

- Use only verified and current firmware (updates).

The following requirements are features of a tested and up-to-date firmware/update:
- Checksum was successfully verified (integrity check).

WAGO recommends using current firmware.

The current version of a firmware corresponds to the current state of the art and security. Previous firmware versions can present vulnerabilities in technology and security.

You can find verified current WAGO firmware (and firmware updates) and information on installation at:
- **https://downloadcenter.wago.com**

For more information, please contact:
- **Technical Support**

Aids

- Use additional tools to check security.

The following tools can help you check the cybersecurity of your system:
- System Logging Protocol (Syslog)

6.3.4 Secure Decommissioning

Secure product decommissioning helps prevent various attacks. Secure decommissioning meets the following requirements at a minimum:
- Deleted data in the product
- Deleted product data in the environment

Data in the Product

- Delete all data saved in the product.

Die folgenden Anforderungen müssen mindestens erfüllt sein:
- Product is reset to factory settings.
- Data that cannot be deleted is overwritten (e.g., with “0”).
- If there is any suspicion that sensitive data has not been deleted: Arrange for scrapping by a disposal service provider qualified in cybersecurity.

Product Data in the Environment

- Delete all data stored by the product in the environment.

Die folgenden Anforderungen müssen mindestens erfüllt sein:
- Product configurations in the configuration environment must be deleted.

6.4 Cybersecurity Capabilities

The cybersecurity capabilities here describe the possible scope of a product type’s cybersecurity capabilities. Not all cybersecurity capabilities described apply to all products of the product type. This example description does not include all cybersecurity capabilities that a product of the given type may have.

For the specific cybersecurity capabilities of a product, see: 🕮 **Product Manual**.

Syslog Protocol

The Syslog network protocol allows event-driven log messages to be transmitted in an IP-based network. They are sent from the client to the server via the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

Access Controls

Access control directs and monitors access to interfaces or data. Only authorized persons can access certain interfaces or data. Various options can be used for access control, such as:

- Access control to the network (e.g., MAC address filter)

User Management

The Webserver has role-based user management. User management can take various forms:

- User accounts can be predefined; then only passwords can be changed.
- User accounts themselves can be set up.

Active Port Indication

Active port indication allows interfaces to be checked and supports detection of unauthorized access. Active ports can be indicated via:

- Optical indicators on the product (LED)

Update Capability

Updates to the software/firmware can be provided that extend the product's features, improve the software/firmware or fix a security vulnerability.

- The product does not come with an automatic update function.

6.5 Cybersecurity Service

Current Security Vulnerabilities

- Learn about current security vulnerabilities.

The following contact points can be used to provide information about current security vulnerabilities:

- Information about known and current security vulnerabilities can be viewed online: "Common Vulnerabilities and Exposures (CVE)," **https://cert.vde.com/de/advisories/vendor/wago/**.
- Information on Schwachstellen of WAGO products is available from the WAGO Product Security Incident Response Team PSIRT **PSIRT**.

Cybersecurity Service Duration

- Find out the duration of the cybersecurity service for your product.

Information on the duration of the cybersecurity service can be found on the product detail page at: **www.wago.com/**<item number>.

List of Figures

List of Tables

Glossary

Attack Vector

Basic mechanism through which cybersecurity attacks can be carried out, e.g., physical access or knowledge of login data

Targets

A specific interface of a product through which cybersecurity attacks of a basic type can be executed. For example, cybersecurity attacks that use physical access as the attack vector can use an address selector switch to disrupt the network.

Targets

Physical or logical object that has value for attackers; example: a memory area with data that is worthy of protection from the operator's point of view

Threat

Possibility of harm to a person or property due to cybersecurity incidents

Vulnerability

A vulnerable spot that is not protected or is insufficiently protected and thus represents a vulnerability.

Subject Index

WAGO GmbH & Co. KG
Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden
✉ **info@wago.com**
www.wago.com

Headquaters	+49 571/887 – 0
Sales	+49 (0) 571/887 – 44 222
Order Service	+49 (0) 571/887 – 44 333
Fax	+49 571/887 – 844169