Industrial Product Security Guideline

System overview with established security practices

Weidmüller

Contents

Safety notes and disclaimer

This guideline does not release you from the obligation to ensure safe handling during usage, installation, operation and maintenance. Each user is responsible for the proper operation of their control system. By using these instructions, you accept that Weidmüller shall not be liable for personal injury or property damage that may arise from such usage.

The descriptions and examples provided do not constitute customer-specific solutions, but are intended solely as an aid for typical tasks. The user is responsible for the proper operation of the products described. This guideline is non-binding and does not claim to be complete with regard to configuration or all possible eventualities. By using this guideline, you acknowledge that we cannot be held liable for damage exceeding the scope of liability described. We reserve the right to make changes to this guideline at any time and without prior notice. In the event of discrepancies between the recommendations in this guideline and other Weidmüller publications, such as manuals, those contents shall always take precedence over this guideline. We accept no liability for the information contained in this document. Our liability, on whatever legal grounds, for damage arising from the usage of the examples, instructions, programs, engineering data, performance data, etc. described in this guideline is excluded.

Safety notes

Devices may fail under unsafe operating conditions and cause uncontrolled operation. Such hazardous events may result in death or serious injury, as well as property damage. Therefore, safety equipment must be provided, such as electrical safety concepts or other redundant safety equipment that is independent of the automation system.

- To protect devices, systems, machines and networks against cyber threats, a comprehensive industrial security concept in line with the state of the art must be implemented and maintained on a permanent basis.
- The operator is responsible for preventing unauthorised access to their plants, systems, machines and networks.
- Systems, machines and components may only be connected to the company network or the internet if the necessary and appropriate protective measures, such as firewalls and network segmentation, have been implemented.

1. Introduction

The rapid digitisation and networking of industrial processes has transformed operational and automation technology (OT). While these advances offer considerable benefits, such as greater efficiency, flexibility and productivity, they also bring serious challenges, one of the most urgent of which is cybersecurity. Cyberattacks on industrial systems are becoming increasingly frequent, and a successful attack can have devastating consequences, including production outages, environmental damage or even loss of life.

As industrial systems become ever more complex and increasingly interconnected, conventional security measures are no longer sufficient. Hackers and other malicious actors actively search for vulnerabilities in OT networks in order to exploit them for disruption or data theft. Organisations in the OT sector must take proactive steps without delay to protect their systems against these threats.

In response to these challenges, regulators in the European Union have introduced a range of cybersecurity regulations that impose new requirements on companies and products. Weidmüller supports this approach with a range of solutions that enhance the security of your machines and plants.

This document provides guidance on building a robust cybersecurity system and integrating Weidmüller components into that system. Throughout, reference is made to the international IEC 62443 standard, which was developed for the cybersecurity requirements of industrial automation systems. This standard provides a comprehensive framework for planning, implementing and maintaining security measures in OT networks.
Weidmüller has certified its secure product development process in accordance with IEC 62443-4-1 and will introduce an increasing number of IEC 62443-4-2-compliant products.

In addition to this guideline, detailed security documents are available for specific product groups. These documents provide quick access to security functions that can be used for planning or carrying out security risk analyses. Product-specific security documents can be found in our **eShop** or in the **Weidmüller Support Center** when you search for your specific product.

www.weidmueller.com/eshop

www.weidmueller.com/support-center

Technical information on the safe use and operation of our products can be found in chapter **3. Defense in depth.**

1.1 The difference between IT and OT

Information technology (IT) and operational technology (OT) are two key areas in industrial companies. Although they are often interconnected and complement each other, they serve different purposes and are subject to different challenges.

IT (information technology) deals with the processing, storage and transmission of data. It supports business processes and administrative tasks through systems such as computer networks, databases and software applications. In IT, security focuses primarily on protecting data against unauthorised access, theft or manipulation. The priorities in IT security are therefore:

- Confidentiality
- Integrity
- Availability

OT (Operational Technology) encompasses the control, monitoring and automation of physical processes and machines in industrial environments. This includes devices such as sensors, actuators, industrial control systems and robots. In OT, the focus is on guaranteeing the continuous operation and security of systems and infrastructures. OT environments require dedicated security solutions that go beyond those used in IT. The security priorities in OT are therefore:

Figure 1: OT security priorities

1.2 The difference between security and safety

Security refers to the protection of digital or physical assets against malicious acts and unauthorised access. This includes protecting computers, networks, software and data against cyberattacks, hacking, malware and other threats. In OT environments, security also extends to protecting industrial plants, production processes and critical infrastructure against damage, sabotage, failures and cyberattacks.

By contrast, **safety** focuses on protecting people, the environment and material resources from hazards and accidents. Safety aims to guarantee the physical well-being of individuals, prevent injuries and avoid industrial disasters or environmental damage.

Both concepts, security and safety, are essential to guaranteeing the overall integrity and reliability of systems. Safety cannot be achieved unless security is also taken into account.

2. Security laws and standards

In the past, security legislation focused primarily on critical infrastructure. Due to the growing threat posed by cyberattacks, new regulations are extending cybersecurity requirements for companies and products across various industries.

Law	Region	Target group	Comments
NIS (Network Information System Security) EU 2016/1148	EU	Asset owners, operators of critical infrastructure	Requires the introduction of a cyber security management system, to be implemented through national legislation in the EU member states
Cybersecurity and Infrastructure Security Agency Act	USA	Asset owners, operators of critical infrastructure	Requires the introduction of a cyber security management system for critical infrastructure

2.1 New and extended security legislation

As cyber threats represent an increasing economic risk, security requirements for companies and products are being significantly extended. The EU is introducing new directives and regulations containing cybersecurity provisions or extending existing legislation.

Directive/Regulation	Mandatory from	Target group	Comments
NIS2 (Network Information System Security) EU 2022/2555	Oct. 2024	Plant operators	Extension of the scope of NIS to additional industrial sectors (e.g. mechanical engineering, electrical engineering) and smaller companies (>50 employees, >€10 million turnover); implementation in national law required
RED DA (Radio Equipment Directive Delegated Act) EU 2033/30	Aug. 2025	Device/machine manufacturers	CE marking requirement for devices with radio interfaces that can communicate directly or indirectly with the internet
Machinery Regulation EU 2023/1230	Jan. 2027	Manufacturers of machinery	CE marking requirement for machinery, new safety requirements
CRA (Cyber Resilience Act) EU 2024/2847	Dec. 2027	Device/machine manufacturers	CE marking requirement for devices or software with digital elements and data communication

2.2 Industry-specific security standards

Some organisations have introduced cybersecurity requirements for specific industries.

Standards issued by organisations	Mandatory from	Target group	Comments
IACS UR-E26/27	July 2024	Ship owners, ship operators	Standards of the International Association of Classification Societies (IACS) requiring cybersecurity systems for new ships

2.3 International security standards

Cybersecurity goes beyond securing individual components; it requires a holistic approach to protecting systems, networks, data and infrastructures at multiple levels. A comprehensive cyber security management system (CSMS) must be in place that defines the requirements for setting up, implementing, maintaining and continuously improving cybersecurity measures. Below you will find the most important international cybersecurity standards.

Standard	Focus	Target group	Comments
ISO / IEC 27001	IT	Plant owners, plant operators	Defines an information security management system (ISMS) with a focus on IT security
ISA / IEC 62443	OT + IT	Plant owners, plant operators, device manufacturers	Defines a cyber security management system (CSMS) for OT and IT that includes requirements for operators, system integrators and component manufacturers

2.4 Standard IEC 62443

The IEC 62443 family of standards comprises a series of international standards and technical reports developed specifically for the cybersecurity of industrial automation systems. The standard was developed by the International Electrotechnical Commission (IEC) to address the specific requirements and challenges of OT systems. In addition, it provides clear guidelines for implementing security controls and procedures in industrial environments.

The standard covers the following aspects:

- Network security
- Security policies and procedures
- Risk management
- Cybersecurity-focused development and maintenance of systems
- Security assessment and certification

Each part of the standard is designed to address different stakeholder groups, such as plant operators, system integrators and component manufacturers. IEC 62443-2-1 provides a mapping to the ISO 27001 standard, which focuses on IT security and enables a comprehensive approach to OT security. IEC 62443 can therefore be used comprehensively for OT security.

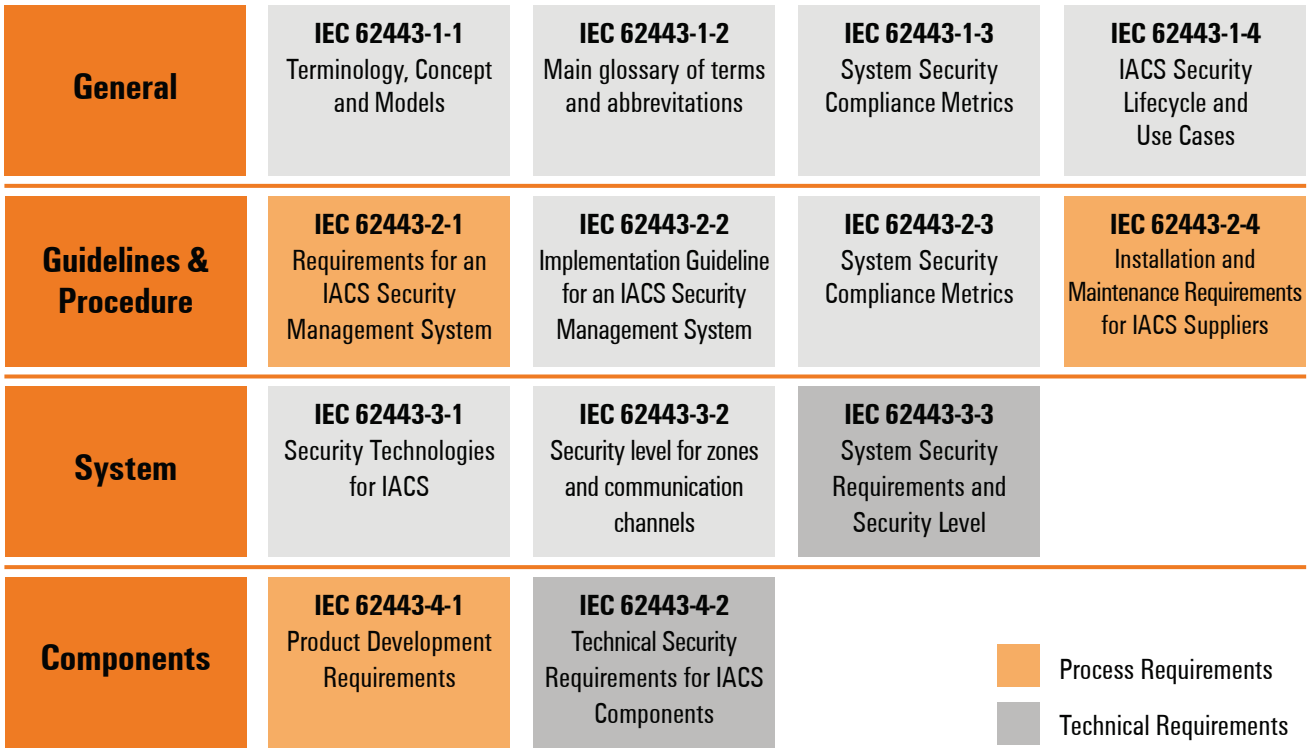


Figure 2: Parts of IEC 62443

The IEC 62443 cyber security management system (CSMS) takes the following core elements into account:

Economic considerations
The business rationale is intended to clarify which business elements are to be protected and how important they are to the company in the event of a successful cyberattack. This includes financial aspects as well as safety, health, environmental and reputational considerations.

Identification, classification and assessment of risks
The cyber risks faced by an organisation are identified, and the likelihood and severity of those risks are assessed.

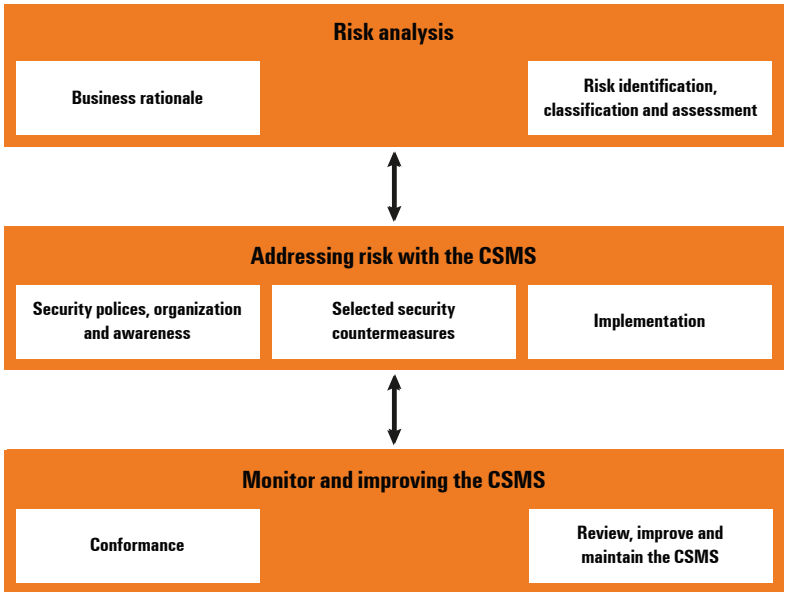


Figure 3: Cyber security management system (CSMS)

Security policies, organisation and awareness
This part addresses strategic and organisational topics such as:
- Scope of the CSMS
- Security organisation
- Employee training and security awareness
- Business continuity plan
- Security policies and procedures

Selected security countermeasures
Definition of security controls for at least the most important elements:
- Personnel security
- Physical and environmental security
- Network segmentation
- Access control

Implementation: Implementation of measures for risk mitigation and achieving security objectives

Compliance: Measures to ensure compliance with the CSMS developed for the organisation

Review, improvement and maintenance of the CSMS: Ensuring on a permanent basis that the CSMS continues to achieve its objectives over time

Compliance at Weidmüller
Weidmüller has implemented a certified secure product development process in accordance with IEC 62443-4-1 and offers secure products in accordance with IEC 62443-4-2.

2.5 Cybersecurity requirements for OT environments

2.5.1 Cyber Resilience Act (CRA)

Although the CRA is valid only within the European Union, organisations outside the EU must also comply with its requirements if they manufacture or supply products for the European market. The CRA focuses on guaranteeing the **cybersecurity of digital products** throughout their entire life cycle, including secure development, deployment and maintenance.

The key points of the CRA are:

- **Scope:** All products with digital elements, including, for example, machines that can be connected to another device or network. Digital elements are hardware and software that process data digitally.
- **Product compliance:** To comply with the Cyber Resilience Act, a product must meet the CRA's cybersecurity requirements. This is achieved by designing and developing products in accordance with the **secure-by-design** principle.
- **Vulnerability management:** Throughout the entire service life of a product, the manufacturer is obliged to maintain vulnerability management for the product and to remedy exploitable vulnerabilities by means of free security updates.

The CRA gives rise to the following key factors for organisations:

- **Cyber security management system (CSMS):** Introduction of a structured management process for achieving cybersecurity
- **Network segmentation:** Dividing the network into zones and conduits in order to limit security risks (e.g. secure zones for critical processes)
- **Device security:** For devices and components used in OT environments, manufacturers must observe the principles of secure by design.

2.5.2 IEC 62443 for OT security

IEC 62443 is a comprehensive cybersecurity standard for industrial automation and control systems. The standard provides a framework for securing OT environments, from plant operators to component manufacturers.

2.5.3 NIST standards (NIST 2.0)

The **National Institute of Standards and Technology (NIST)**, through its standards, provides a cybersecurity framework that is used in many North American industries, including critical infrastructure and OT environments. Version NIST 2.0 focuses on proactive security measures and improving resilience against cyberattacks.

The key NIST 2.0 elements for OT are:

- **Identify:** Understand and catalogue OT assets and risks.
- **Protect:** Implement security measures such as firewalls, VPNs and secure authentication.
- **Detect:** Monitor OT environments for potential threats using intrusion detection systems (IDS).
- **Respond:** Create incident response plans tailored to OT-specific scenarios.
- **Recover:** Ensure that disaster recovery and business continuity plans are in place.

2.5.4 Comparison of requirements

Standard	Focus	Applicable areas
CRA	Security in the digital product life cycle	Manufacturers of OT devices and software
ISA / IEC 62443	Cybersecurity for OT environments	Plant owners, integrators and component manufacturers
NIST 2.0	Comprehensive cybersecurity framework	Plant owners and critical infrastructure providers

3. Defense in depth

The security concept of **defense in depth** is a strategic approach aimed at protecting systems and networks against a wide range of threats by implementing multiple layers of security. This concept is based on the understanding that a single security measure is not sufficient to protect a system completely. Instead, several levels or layers of security are implemented in order to detect, prevent or mitigate potential attacks at different levels.
Defense in depth is a multi-layered strategy that integrates people, technology and operational capabilities to establish variable barriers across multiple levels and dimensions of the organisation.

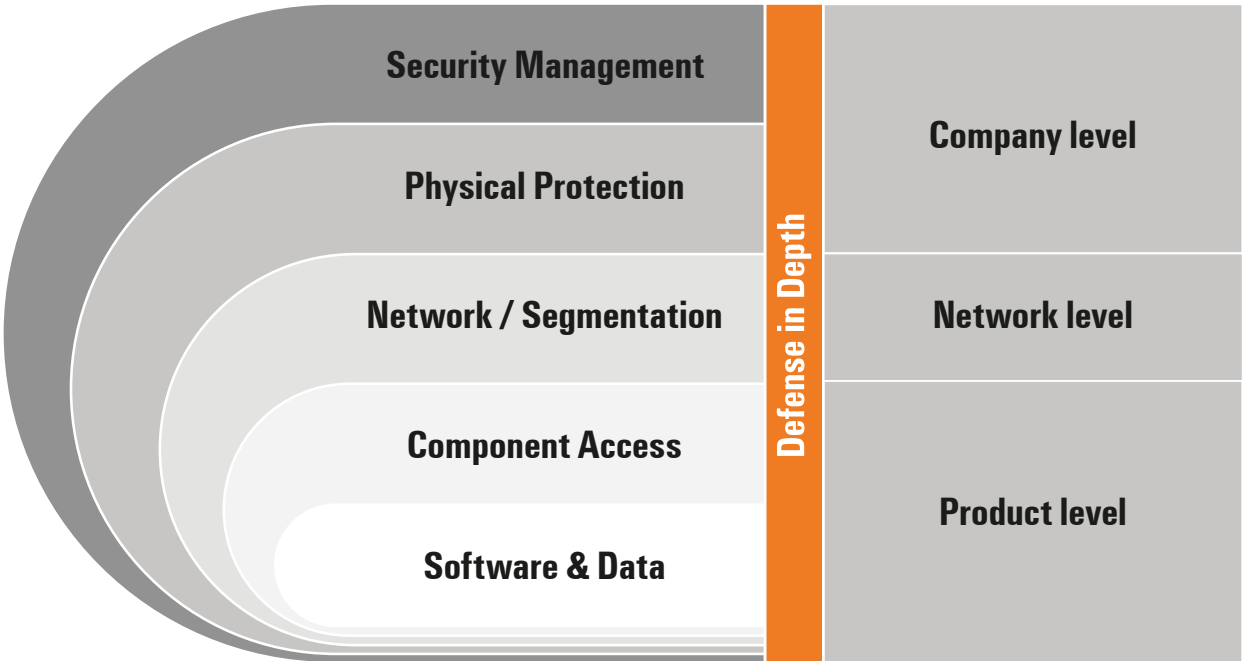


Figure 4: Layered model of defense in depth

The following sections describe the individual layers and how you can use Weidmüller components to build a security system.

3.1 Defense-in-depth layer: Security management

Security management is an overarching cybersecurity programme that supports the protection of the OT environment. This layer addresses organisational topics by setting up a cyber security management system (CSMS). This includes policies, processes and awareness-raising. The regulations and processes of security management guide and influence the other defense-in-depth layers in the decisions that need to be made.

Typical topics at this layer include:

- Staff awareness and training
- Definition and review of the responsibilities of all plant users
- Definition and review of user roles
- Definition and review of user access rights
- Control of physical access
- Implementation of an incident response plan for actions to be taken following a security incident
- Definition of a patch management system for the distribution of security patches

3.1.1 PSIRT

PSIRT stands for **Product Security Incident Response Team**. A PSIRT is a specialised team within a company or organisation that deals with the remediation of security incidents affecting products or software. As soon as security gaps or vulnerabilities in a product are discovered, the PSIRT is responsible for investigating, assessing and remedying them. In addition, a PSIRT communicates with customers, suppliers and other relevant parties in order to share information about security issues and offer solutions.
Weidmüller has established a PSIRT and uses the **Security Advisory Board** on the Weidmüller website to provide information on product-specific security vulnerabilities and their remediation.

www.weidmueller.com/security-advisory-board

In addition, Weidmüller publishes security vulnerabilities in its products via **CERT@VDE**, a neutral, non-profit platform. CERT@VDE supports its partners in matters relating to the cybersecurity of products in the automation industry in order to enable the rapid, structured and professional handling of security vulnerabilities.

www.cert.vde.com

3.1.2 CSIRT

CSIRT stands for **Computer Security Incident Response Team**. Unlike a PSIRT, a CSIRT focuses not only on products, but also on an organisation's general IT infrastructure. A CSIRT is responsible for the detection, remediation and management of security incidents in a broader context.

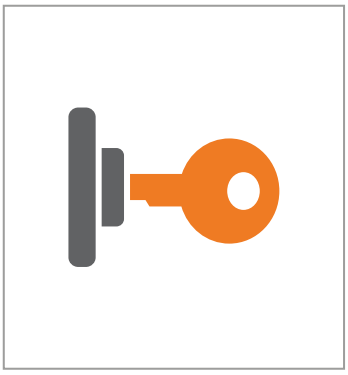
3.2 Defense-in-depth layer: Physical protection

Physical security measures are intended to reduce the risk of accidental or deliberate loss of or damage to assets and the surrounding environment.

- Keep the group of people with access authorisation as small as possible.
- Equip cabinet doors with access protection, e.g. keys.
- The lockable FrontCom Vario system from Weidmüller is suitable as a secure, externally accessible service interface.

General Access Control

Cabinet lock with key



Lockable Service Interfaces Weidmüller FrontCom Vario

Figure 5: Examples of physical access systems

Weidmüller components are intended for use in industrial environments. Weidmüller IP20 components are designed for operation in a protected enclosure. Physical access to the devices must be granted only to authorised persons.

3.3 Defense-in-depth layer: Network segmentation

The network is a primary target for cyberattacks. An essential countermeasure is network segmentation, as it ensures that any potential attack remains confined to a limited area.

Basic principles of network segmentation (zones and conduits)

a. Avoid large zones: Large zones can create vulnerabilities. If you keep zones small, you can contain potential threats more effectively.
b. Define hierarchical zones: Establish zones with the same security level in order to simplify management and increase security.
c. Secure transitions (conduits): Ensure that the transitions between zones are well protected. Use firewalls to restrict communication to what is necessary.

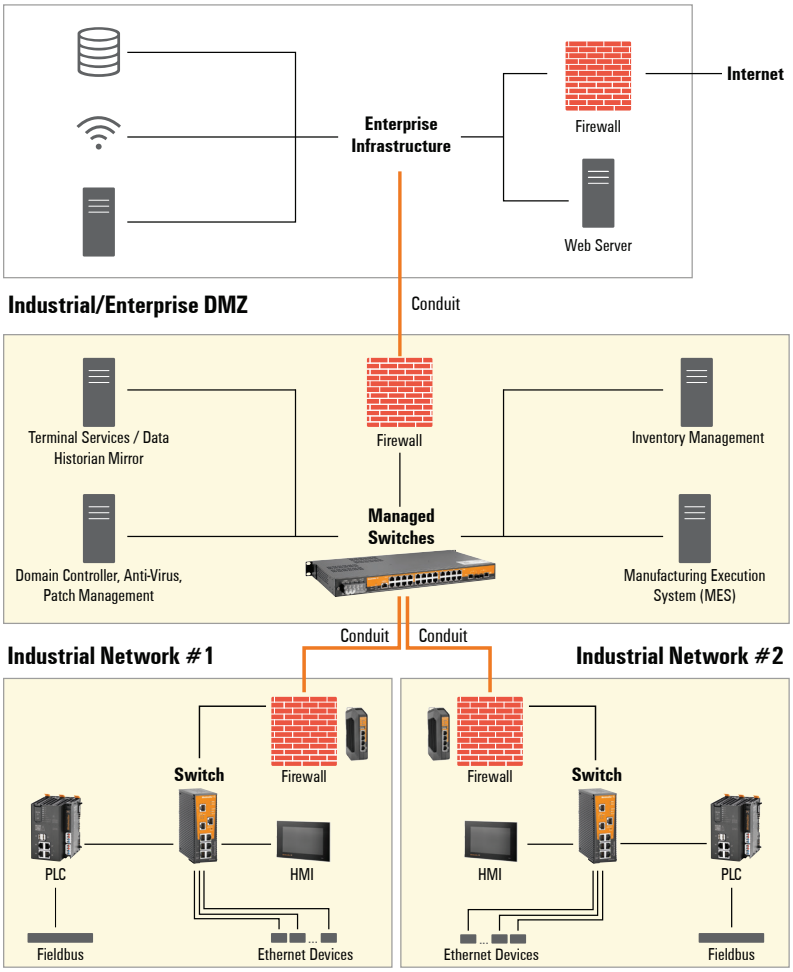


Figure 6: Network architecture with zones and data connections (conduits)

Zone: Yellow segment. A group of components with the same security level.

Conduit: Orange line. Protected channel for data exchange.

Normally, a router uses its firewall to protect a conduit so that only the necessary communication is permitted. Communication in a conduit should be encrypted wherever possible. If the protocol used does not provide for this, a secure channel (via VPN tunnels) or secure encrypted communication, e.g. HTTPS, OPC UA, should be used.

There are various system concepts for zones and conduits, as shown in the figure. Each company must decide individually on the optimum architecture, even if the basic principles are identical.

DMZ stands for **Demilitarised Zone** and refers to a specially controlled network located between the external network (internet) and the internal network, or between two critical internal networks. The DMZ is a buffer zone that separates the networks from one another through strict communication rules and firewalls.

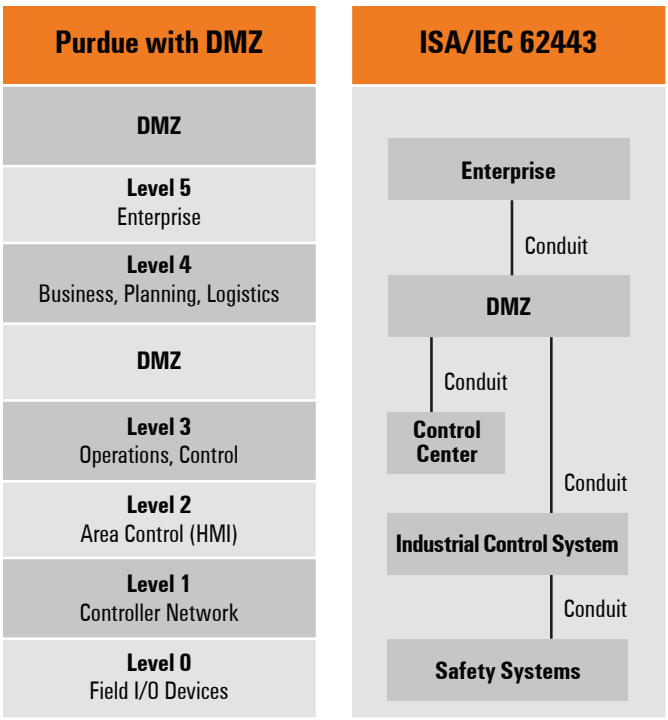


Figure 7: Different zone concepts

Example of the automation structure of a machine and the OT network infrastructure of the factory hall using Weidmüller components.

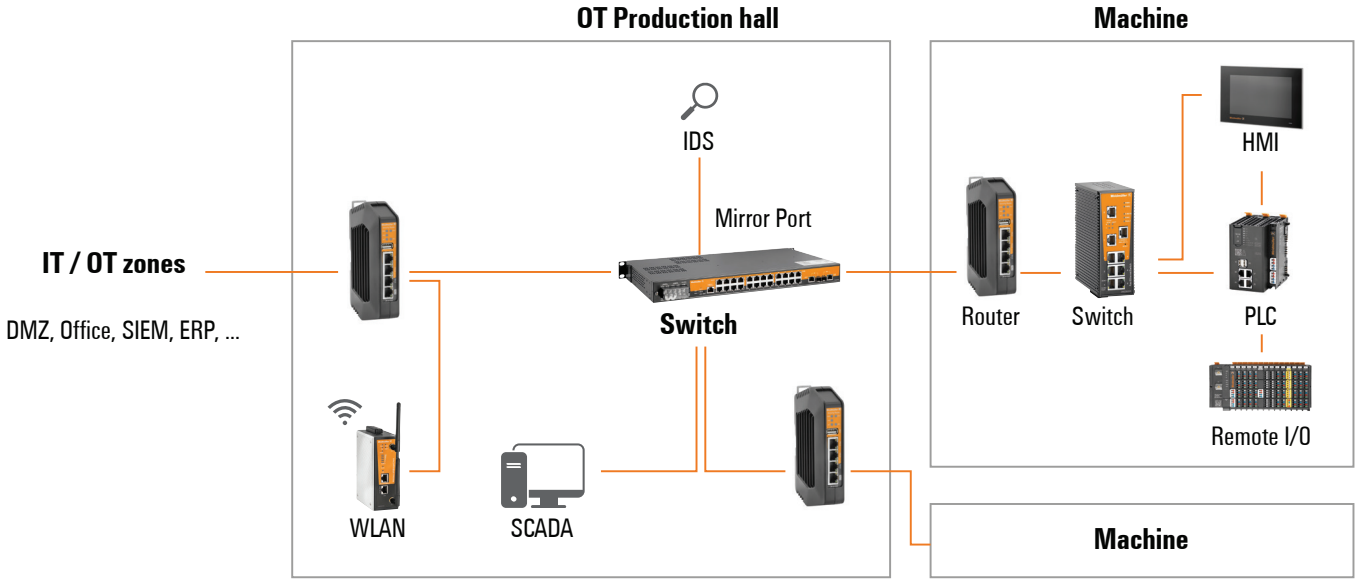


Figure 8: Example of a network segmentation structure

Established security practices for network segmentation

- **Segment networks:** Segment the network into zones with the same security level. Create zones within machines and the OT area using routers, VLANs or layer 3 switches.
- **Set up firewalls:** Protect your computers with routers equipped with firewalls, either integrated or positioned externally.
- **Protect fieldbus networks:** Implement physical access controls for fieldbus segments, as fieldbus networks have a low security level.
- **Isolate Wi-Fi networks:** Use separate VLANs for Wi-Fi access, combined with robust security measures such as firewall rules and centralised access management (e.g. IEEE 802.1X).
- **Consider intrusion detection systems (IDS):** Use IDS to monitor attacks and use mirror ports of a managed switch for traffic analysis.

3.3.1 Switches and VLANs

A VLAN (Virtual Local Area Network) is a logical network established within a physical network. A VLAN enables the segmentation and organisation of devices in networks regardless of their physical location.

Traditionally, devices in a network are segmented by means of physical connections. VLANs, by contrast, enable devices in a network to be grouped according to logical criteria such as function, department, application or security level, regardless of their physical location in the network. This segmentation provides greater flexibility, security and more efficient use of resources.

Weidmüller Managed Switches offer port-based VLAN and tagged VLAN support for logical network segmentation. This makes it possible to set up network segments with different security levels within the machine, the production line or the plant.

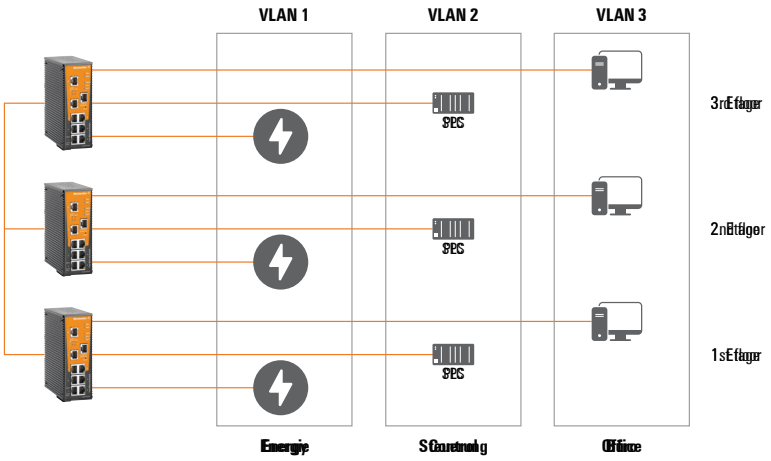


Figure 9: VLAN segmentation

A typical example of a VLAN is the logical separation of an energy monitoring network (e.g. Weidmüller energy meters using Modbus TCP) from a production-relevant network. Both networks use the same physical network, so no additional cabling is required.

You can also use Weidmüller Ethernet switches in combination with fieldbus systems such as PROFINET or EtherNet/IP. Please note the technical data of the switches.

Further information on fieldbus security can be found in chapter **3.3.3 Fieldbus network**.

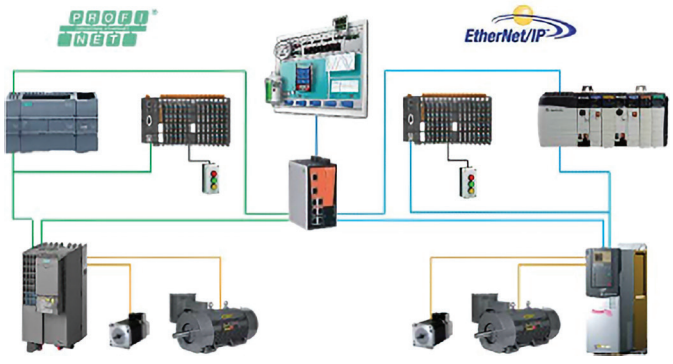


Figure 10: Fieldbus network with switch

Established security practices for switches and VLANs

- **Implement VLANs:** Use VLANs to segment networks according to security criticality (e.g. separate Wi-Fi access points or energy meters).
- **Secure user interfaces:** Disable HTTP and use HTTPS for web interfaces. Disable TELNET in favour of SSH for CLI access. Optionally set the switch's management VLAN ID to a separate VLAN so that the switch web interface can only be reached via a separate VLAN (e.g. only one port in the network system).
- **Restrict SNMP usage:** Disable SNMP if it is not used. If required, use SNMPv3 with a secure password.
- **Disable unnecessary services:** Disable all unnecessary services (e.g. PROFINET, ...) in order to reduce potential attack vectors.
- **Block unused ports:** Disable unused physical ports by means of port blocking functions.
- **Static MAC address binding:** Use MAC or IP address binding to restrict network access.
- **Implement access control lists (ACLs):** Configure ACLs to control network traffic.

3.3.2 Routers

Network routers with firewalls are important components of network security. They control, segment and filter data traffic in order to minimise potential threats and guarantee the protection of sensitive resources. Routers offer the following typical functions:

Network segmentation: Routers can be used to divide a network into several physical segments or subnets. By controlling traffic between different segments, routers can enforce security policies and restrict access to sensitive areas.

Firewall functions: Modern routers have integrated firewall functions that can monitor and filter incoming and outgoing traffic. This makes it possible to block unwanted traffic and detect and prevent potentially harmful activities. In addition, data protection is improved by controlling access to certain services or resources.

NAT (Network Address Translation): Routers use NAT to convert private IP addresses in the internal network into public IP addresses when communicating in the higher-level network (or internet). This provides a certain degree of security, as internal network addresses are protected against disclosure to external networks. This can reduce the attack surface and protect the privacy of internal network resources.

VPN (Virtual Private Network): Routers can provide VPN functions to establish secure connections between remote locations or users. VPNs encrypt data traffic and enable secure communication over insecure networks such as the internet. This also allows remote users to access company resources without compromising security.

Established security practices for routers

- We demonstrate the secure configuration of a router in this video:

  www.weidmueller.com/secure-router-configuration

- Change the firewall settings (packet filter): Weidmüller Industrial Security Routers feature a powerful whitelisting firewall. This means that any communication that does not match a rule from top to bottom is discarded. The routers contain one factory-set firewall rule: "Allow All". To improve security, create a list of the communications routed through the router. Then add these communication parameters to the firewall settings for a whitelist. Once all required traffic has been fully listed, delete the "Allow All" rule to ensure that all remaining traffic is blocked.
- Apply access restrictions: Various user profiles with different permissions can be created on Weidmüller Industrial Security Routers.
- Grant access only to those who need it, and only with the rights they need for their tasks.
- Secure user interfaces: Disable HTTP access to the router on all interfaces.
- Access via a public network: Disable HTTPS access to the router on interfaces exposed to a public network (WAN / mobile WLAN) if this is not required. Use VPN for communication with the public network.
- Restrict SNMP usage: SNMP is disabled by default. If you use it, make sure that you use SNMPv3 and choose a secure password instead of the default password.
- Use VPN for insecure networks: A Virtual Private Network (VPN) is recommended for remote access to your local network segment (via an insecure network).
  On the Weidmüller Security Router, this can be done via an open technology such as OpenVPN or IPsec or via the Weidmüller u-link Remote Access Service.
- Further information can be found in chapter **3.3.4 Remote access**.

3.3.3 Fieldbus network

Fieldbuses such as PROFINET, EtherNet/IP, EtherCAT, Powerlink, CANopen or Modbus are optimised in terms of real-time communication for low cycle times, minimal jitter and data consistency. Encrypted data transmission is not provided in this real-time communication. In addition, the configuration parameters are often transmitted unencrypted from the controller to subordinate systems such as remote I/O (e.g. u-remote).

Proprietary or web browser-based configuration tools are frequently used for engineering the controller and fieldbus configuration and for controller-independent configuration of fieldbus devices. Access to the device can be via a separate service interface or directly via the fieldbus (depending on the fieldbus).
Weidmüller devices with a web browser interface are protected against unauthorised access by user management (see chapter 3.4 Defense in depth layer: Component access).

According to the current state of the art, we recommend separating the controller and plant network from other networks within an operational network infrastructure. In addition, we recommend strict access control for such machine and plant sections.

Established security practices for fieldbus networks

- **Restrict physical access:** Secure access to fieldbus networks with physical access controls.
- **Separate networks:** Separate the fieldbus network from other networks.
- **Create small segments:** Segment large fieldbus networks into smaller units in order to confine a potential cyberattack to a smaller area.
- **Secure transitions:** Secure communication transitions to other zones by means of routers with appropriately configured firewall rules.
- **Use fixed IP addresses:** Assign fixed IP addresses to devices and avoid the use of DHCP services.
- **Use HTTPS:** Use secure HTTPS communication instead of HTTP.
- **Disable web server access via the fieldbus:** To minimise the risk of cyberattacks, some u-remote fieldbus couplers offer the option of preventing web server access via the fieldbus. Web server access is then possible only via USB. Where possible, disable fieldbus web server access.
- **Fieldbus documentation:** Follow the fieldbus-specific documentation to guarantee operation is as secure as possible.

3.3.4 Remote access

Remote access allows users to connect to a network or device from a remote location, often via a virtual private network (VPN). Although this can increase productivity because work is possible from different locations, a VPN also poses security risks if it is not properly secured.

Important considerations:

- Security risks: Attackers can use remote access to gain unauthorised access to sensitive systems and data. Robust security measures are therefore essential.
- Cooperation: A clear agreement should be reached between the machine manufacturer and the operator regarding the scope of remote access. For critical interventions, personnel should be present on site and access should be granted by means of local authorisation.

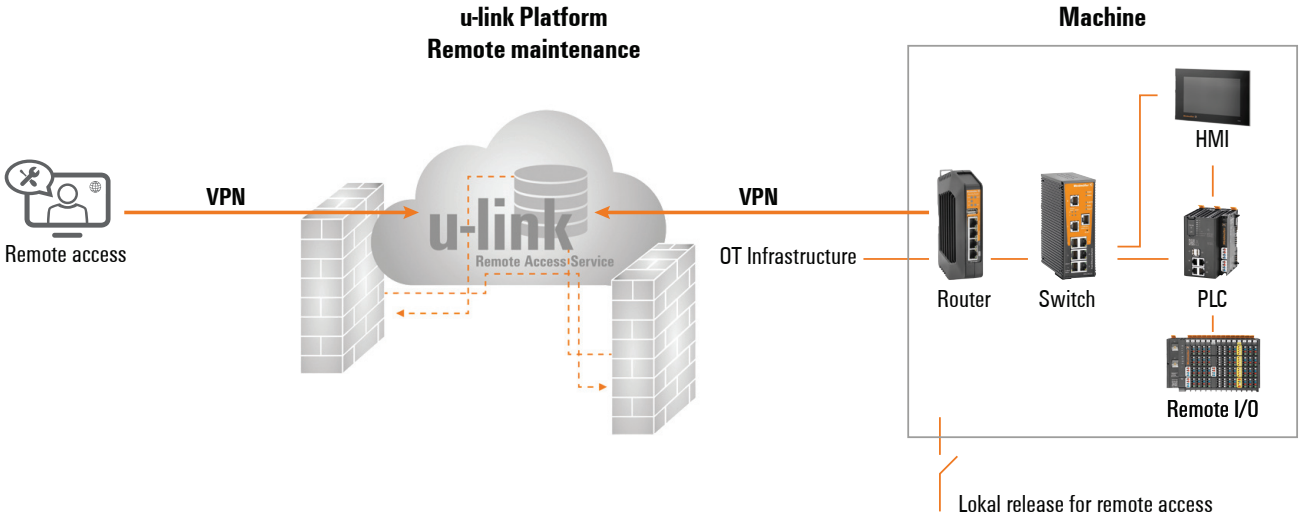


Figure 11: Remote access service with u-link

Weidmüller u-link system

With u-link, Weidmüller offers a secure remote access solution:

- A central cloud platform
- u-link-enabled devices (e.g. security routers, PLCs, IoT gateways)
- Customer access via service computers or portable devices

The u-link platform complies with ISO 27001 standards and has robust security features, including:

- Multi-factor authentication (MFA)
- User management with user roles and rights
- Secure VPN communication
- Logging of user activities

Established security practices for remote access

- **Secure VPN:** Implement a securely encrypted VPN connection, such as Weidmüller u-link, to protect data during remote access.
- **Multi-factor authentication (MFA):** Implement MFA to increase the security of remote access services. u-link offers MFA options.
- **Principle of Least Privilege (PoLP):** Configure user rights so that each person has only the permissions required for their task. This principle also includes defining which devices and ports can be accessed.
- **Agreement on the scope of remote access:** Reach a clear agreement on remote access between the machine manufacturer and the operator before access is granted.
- **Local authorisation for remote access:** Use physical switches or similar methods to allow or deny remote access. Weidmüller u-link routers have a digital input for controlling remote access on the basis of local authorisation.
- **Prepare software updates:** Make sure that the machine or system is in a safe state before transferring and installing software updates.

3.4 Defense-in-depth layer: Component access

Access to information on a device is referred to as user management. Alternatively, the following terms are also commonly used:

- Access management
- IAM (Identity and Access Management)
- User and permission management

User management comprises the following core elements:

- Identification: Assignment of a unique identity to each user within the system (e.g. user names).
- Authentication: Verification of the identity of users (e.g. by means of passwords or other verification methods).
- Authorisation: Definition of which functions and resources an authenticated user can access (e.g. permission to make configuration changes).

All Weidmüller devices with a web browser interface have user management to protect against unauthorised changes. Permissions can be defined with varying degrees of granularity, depending on the device. User management is a crucial element of security protection and should be used diligently in accordance with the relevant security requirements.

3.4.1 Strong password

A password strength of at least 8 characters, including lower-case and upper-case letters, digits and special characters, is recommended.
We recommend using a password length of at least 20 characters with 2 character types. If only one character type is used, the password length should be at least 25 characters.

Example: u-remote requires 3 different character types.

3.4.2 Principle of least privilege

The principle of least privilege states that each user should be granted only the permissions required to perform their tasks. This concept is intended to minimise security risk by reducing potential attack surfaces.

Administrators must therefore carry out a thorough analysis of tasks, roles and responsibilities within the organisation before setting up user rights. In addition, all permissions should be reviewed regularly and adjusted where necessary.

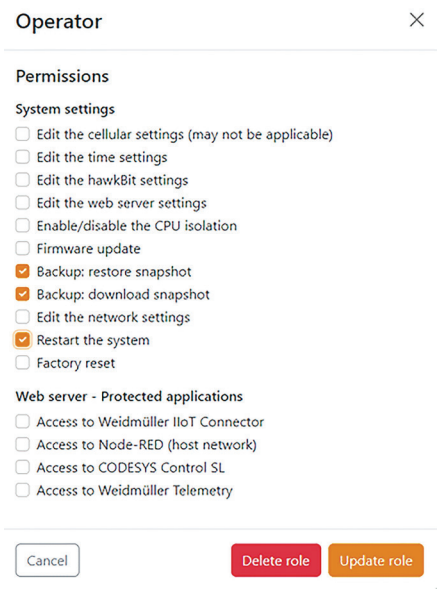


Figure 12: Definition of access rights in u-OS

3.4.3 Browser warnings

When you connect your web browser to the Weidmüller device, you will often receive a browser warning such as “insecure connection”, “your connection is not private” or a similar message. This is due to your browser’s security settings or the self-signed certificate on the device.

Here is an example from a Chrome browser:
The reason for the use of self-signed Weidmüller certificates is that a certificate is bound to the IP address used. As this address is typically adapted to the application, the user must also issue a customised certificate. Further information on this can be found in the following chapter.

To communicate with the Weidmüller device, click on “Advanced” or the equivalent and select the option indicating that you want to communicate with the device in an insecure manner.

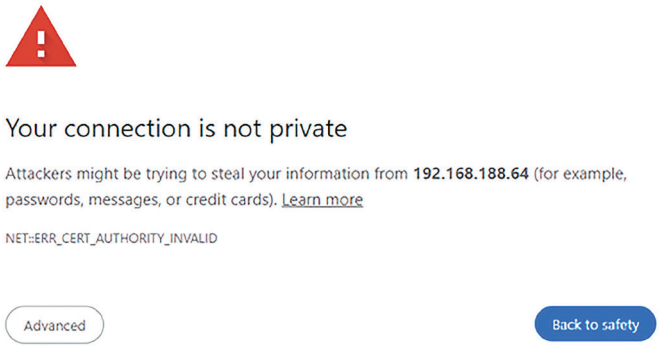


Figure 13: Possible browser message

3.4.4 Creation and exchange of certificates

A certificate enables a secure communication connection via HTTPS. The green padlock symbol in the browser indicates that this website has a valid and trusted certificate and that the connection is secure.
It is recommended that the existing Weidmüller certificates be replaced with your own certificates.

Specially created certificates can be signed by a certification authority (known as a root CA). The root certificate forms the common trust anchor for all subordinate certificates and must be stored in the local trust store of the browser or client. In machinery and plant engineering, however, this is often too time-consuming.

Alternatively, self-signed certificates can also be used. The XCA key management software can be used for this purpose. It is important that the database file used is specially protected so that the private keys do not fall into unauthorised hands.

Select the RSA key type and a key length of 4096 bits.

A **video tutorial** on creating self-signed certificates can be found in the Weidmüller Support Center.

www.weidmueller.com/creating-certificates

Established security practices for component access

- **Use an HTTPS certificate:** Create your own certificate for HTTPS communication (see above).
- **Application of the principle of least privilege:** Apply the principle of least privilege described in chapter 3.4.2.
- **Change the password:** Change the default password during the initial configuration of the device.
- **Use a secure password:** Use a secure password; see chapter 3.4.1 Strong password.
- **Use specific passwords:** Do not use the same password for multiple applications.
- **Use individual users:** A unique identifier (freely selectable name) for each user is recommended.
- **Secure management interfaces:** Disable HTTP and enable HTTPS access to the device for interfaces with user interaction.

3.5 Defense-in-depth layer: Software and data

This defense-in-depth layer covers security topics located in the respective device and primarily relating to the handling of software and data.

These include:
- Firmware and its updates
- Apps and their updates
- Applications
- Data backup and restore
- Logging

3.5.1 Firmware and updates

Weidmüller uses specially hardened industrial operating systems in its devices and provides software updates for its products. Please check our **Support Center** regularly to see whether new updates are available for your product.

www.weidmueller.com/support-center

Updates can be loaded into the device manually via the web user interface.

For Weidmüller Security Routers, new firmware can also be installed on the connected routers via the central u-link cloud platform. The user is shown whether an update is available for the router. This update can be installed on the device either directly or on a scheduled basis.

For devices with the u-OS operating system, Weidmüller offers, in addition to manual updating via the web user interface, an automated update function called rollout management. Rollout management is integrated into the Weidmüller easyConnect platform. It uses the open-source software Hawkbit, which also allows an alternative server operation directly within the company network.

Established security practices for firmware and updates

- **Use secure sources:** Download updates only from trusted sources, e.g. the Weidmüller Support Center.
- **Search for updates:** Check regularly for new updates for the devices you use.
- **Install security updates promptly:** Install software updates and security fixes as quickly as possible.
- **Perform updates only when the machine is in a safe state:** Bring the machine or system into a safe state before updating.
- **Service personnel present:** Ensure that service personnel are present at the machine or plant while an automatic update is being carried out so that action can be taken in the event of a security incident.
- **Test updates:** Test the new software before installing it on a large scale.

3.5.2 Backup and restore

Backup and restore are extremely important in the context of a security management system for the following reasons:

- Data recovery after a security incident
  If a security incident such as data loss, a ransomware attack or a system failure occurs, backups can be used to restore the affected data. This minimises the damage such an incident can cause and enables the company to resume operations quickly.
- Protection against data loss
  By performing regular backups, a company can ensure that its data is stored securely and can be restored in the event of a problem. This significantly reduces the risk of permanent data loss.
- Compliance requirements
  Many industry-specific requirements and laws require companies to create backup copies of their data and retain them for a certain time interval in order to guarantee the integrity and availability of the data.
- Protection against ransomware
  In the event of ransomware attacks, backups protect a company from having to pay ransom to recover its data. Anyone with up-to-date and intact backups can restore the data without having to give in to the attackers.
- Recoverability after human error: People make errors, whether by accidentally changing or deleting files or unintentionally changing settings. Backups make it possible to restore data from an earlier state and thus correct human errors.
- Business continuity
  Backups play an important role in maintaining business continuity. If an unexpected event occurs that impairs access to data, backups can be used to maintain business operations while the problem is being resolved.

Weidmüller devices support backup and restore functions. The procedure is described in the relevant device manual.

Established security practices for backup and restore

- **Regular backups:** Perform regular backups of your devices.
- **Secure storage:** Store backups in a secure location.
- **Long-term storage:** Keep backups for an extended time interval. Malware may have infected the system long before the attack was detected.
- **Check the recovery process:** Regularly check the restore function to ensure that the backup and restore process works properly.

3.5.3 Logging

Logging is an essential function in a security environment for monitoring, analysing and responding to security incidents, and helps to improve the security and compliance of systems and networks.

Logging offers the following benefits:

- Event tracking:
  Logs contain a detailed record of events occurring in a system or network. These events may include attacks, unauthorised access, failed login attempts and other suspicious activities. By analysing logs, security teams can identify and respond to potential security incidents.
- Forensic analysis:
  Logs are essential for the forensic analysis of security incidents. Using the logged information, security analysts can reconstruct the course of an attack, identify affected systems and assess the extent of the damage.
- Compliance with regulations:
  Many security regulations and standards require certain events and activities to be logged. Through logging, organisations can ensure that they meet the requirements of compliance guidelines.
- Early detection of threats:
  Continuous monitoring of logs makes it possible to identify potential security threats at an early stage. Anomalies in the behaviour of users, systems or applications may indicate potential security incidents that require further investigation.
- Auditing and traceability:
  Logs are also used to review user activities and system operation. Organisations can trace who accessed which resources, which actions were carried out and when they took place. This is the only way to guarantee the integrity and confidentiality of data.

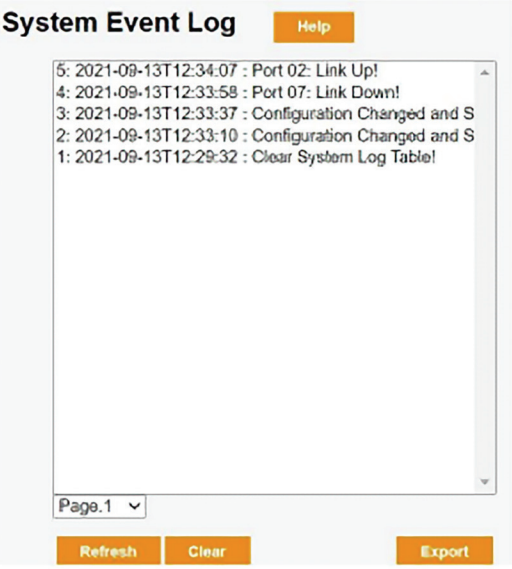


Figure 14: Example of an event entry

Established security practices for backup and restore

- **Use logging:** Use the logging functionality in your Weidmüller device (event logging).
- **Connection to a SIEM system:** Ideally, use a central SIEM system for your OT area. Activate the SYSLOG function in your Weidmüller device and use a VPN connection to the SIEM server (SYSLOG is UDP-based).

3.5.4 u-OS apps and updates

The Linux-based u-OS operating system for u-control and IoT gateway products allows the system to be individually extended via Docker containers or SSH access (SSH = Secure Shell).

Weidmüller offers its own Docker containers and those of third-party providers as ready-made apps that can be loaded onto the device and run there.

The "Portainer.io" app is available for the initial installation and for updates of self-developed Docker containers. Weidmüller uses specially hardened industrial operating systems in its devices.

Established security practices for apps and updates

- **Use secure sources:** Download updates only from trusted sources (e.g. Weidmüller APPHUB or Weidmüller Support Center).
- **Search for updates:** Check regularly for new updates for the devices you use.
- **Install security updates promptly:** Install software updates and security fixes as quickly as possible.
- **Perform updates only when the machine is in a safe state:** Bring the machine or system into a safe state before updating.
- **Test updates:** Test the new software before installing it on a large scale.
- **Service personnel present:** Ensure that service personnel are present at the machine or plant while an automatic update is being carried out so that action can be taken in the event of a security incident.
- **Risk analysis:** Create or update your security risk analysis.

3.5.5 CODESYS

The CODESYS app extends the u-OS device with real-time control functionality and real-time communication with various fieldbuses. In addition, communication with higher-level systems such as servers or cloud applications is enabled.

PC-based engineering with the CODESYS app and the corresponding interfaces to the device creates additional attack vectors that must be addressed through the application of the security functions described below.

CODESYS is a partner product of the CODESYS Group. Further information can be found at **www.codesys.com**

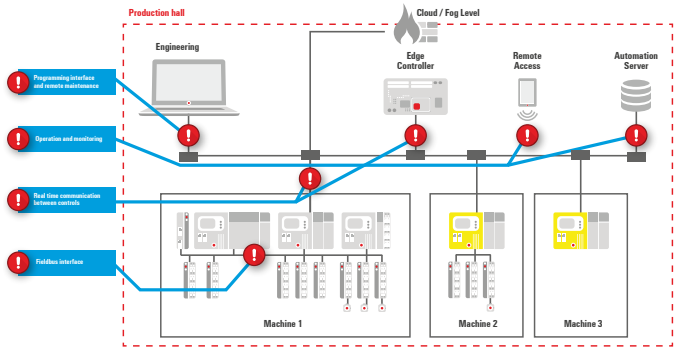


Figure 15: Main attack vectors for an automation system

The CODESYS system offers the following security functions:

CODESYS development system
- Encryption of the application source code using a password, a dongle or X.509 certificates.
- User management at project level
- Encrypted communication between the CODESYS development system and the PLC

CODESYS runtime system
- User management for access to the controller
- Encryption and signing of the executable application code
- Operating modes for the executable application code
- Interactive login on the target device
- Simple replacement or restoration of controllers
- Encrypted OPC UA communication

Application code
- Access restrictions via the application
- Activate additional functions. Define in detail which users are authorised to execute or operate specific functions of the application.

Visualisation
- User management for visualisations
- Encrypted communication for CODESYS WebVisu

CODESYS Automation Server
- Encapsulation of devices in the local network: Data exchange with the server exclusively via the CODESYS Edge Gateway
- Encrypted communication: Data exchange between the server and the CODESYS Edge Gateway is end-to-end encrypted via TLS based on X.509 certificates.
- Reliable user and rights management: Access to objects and information can be fine-tuned, e.g. via object properties and user accounts, with the latter additionally protected by two-factor authentication.
- Complete transparency of actions: Recording of access and changes via audit trail
- Know-how protection: Signing/encryption of source code and compiled binary code using an X.509 certificate, dongle or password
- Certified security: Regular security audits by external auditors

CODESYS security notes

www.codesys.com/security

3.5.6 Weidmüller software tools

Weidmüller also offers the PROCON software family and ResMa. These software tools can be installed on third-party Windows and Linux devices. To guarantee secure operation, the following instructions must be observed.

Established security practices for Weidmüller software

- **Secure the host system:** The PROCON-WEB SCADA and ResMa software tools are designed for use on Windows devices. PROCON-WEB Embedded and PROCON-Connect are designed for use on Windows and Linux. The operating system must be secured in order to guarantee the integrity of all configurations and data stored on the device.
- **Use HTTPS instead of HTTP:** Unlike ResMa, PROCON-WEB does not use HTTPS by default. It is recommended that HTTPS be enabled in the configuration to allow encrypted communication.
- **Change default passwords:** Change the default passwords for admin and streaming immediately after installation.
- **Configure secure password policies:** To guarantee secure passwords, configure the password policies in accordance with our recommendation; see chapter 3.4.1 Strong password.
- **Set up user management:** Use user and permission management when creating HMI software. Protect your HMI with the integrated user management and use permissions in your project to protect different actions and views with different permission levels.
- **Principle of least privilege:** When creating permission sets for different roles, make sure that only the required permissions are assigned.
- **Install security updates:** If Weidmüller provides information about security vulnerabilities in the software, it is strongly recommended that the security patch provided be installed.

4. Glossary

Term	Explanation
Conduit	A conduit groups together the elements that enable communication between two network zones. Conduits provide security functions for secure communication and for the coexistence of zones with different security levels.
CRA	**Cyber Resilience Act** EU regulation for products with digital elements and communication functions.
CSIRT	**Computer Security Incident Response Team** The CSIRT is responsible for vulnerability management at system level; see also PSIRT at product level.
CSMS	**Cyber Security Management System** Term from IEC 62443 for the overall security management system. The similar term from ISO 27000 is ISMS.
CSRS	Cybersecurity Requirements Specification
DMZ	**Demilitarised Zone** A DMZ network is an additional layer of security that enables companies to separate private networks from public internet access and protect important data.
DoS / DDoS	**(Distributed) Denial-of-Service attack** A DoS attack is a cyberattack with which the attacker seeks to prevent users from accessing network or computer resources.
ENISA	**European Union Agency for Cybersecurity** Agency of the European Union for cybersecurity
IACS	**Industrial Automation and Control System** Term from IEC 62443. IACS consist of hardware, software and network components used for the automation and monitoring of industrial production plants and their processes.
IDS	**Intrusion Detection System** An IDS automatically detects attacks on computer systems or networks on the basis of certain patterns and informs users or administrators.
IEC 62443	IEC 62443 is an international series of standards on “Industrial communication networks – IT security for networks and systems”. The various parts of the series describe both technical and procedural aspects of industrial cybersecurity. The series divides industry into different roles: operators, integrators and manufacturers.
IEC 62443-3-3	This part of the IEC 62443 standard defines the system requirements for a secure system and describes 5 security levels (4 levels with security functions; level 0 without security).
IEC 62443-4-1	This part of the IEC 62443 standard defines what a secure product development process should look like; see also SPDL.
IEC 62443-4-2	This part of the IEC 62443 standard defines the product requirements for a secure product and describes 5 security levels (4 levels with security functions; level 0 without security).
ISA 62443	The series of standards published by the International Society of Automation (ISA) defines requirements and procedures for the implementation and maintenance of electronically secure industrial automation and control systems (IACS). ISA 62443 is identical to IEC 62443.
ISMS	**Information Security Management System** Term from ISO 27001. This term is synonymous with the term CSMS in IEC 62443.
IT	**Information Technology** Abbreviation for the classic IT infrastructure such as MS Office, ERP, email and web servers.
NIS / NIS2	**Network and Information Security** Term from EU law. NIS covers critical infrastructure only. NIS2 has an extended scope covering many other industrial sectors. NIS2 enters into force through national legislation.
NIST	**National Institute of Standards and Technology** The institute is a non-regulatory agency within the US Department of Commerce that drives innovation by advancing science in the fields of measurement, standards and technology.
NIST CSF	**NIST Cybersecurity Framework** The NIST CSF is one of the most widely used security frameworks in US industry.
OS	**Operating System**, e.g. Weidmüller u-OS

Term	Explanation
OT	**Operational Technology** Infrastructure in the production environment with production machines and production IT infrastructure
PKI	**Public Key Infrastructure** A public key infrastructure is a hierarchical system for the generation, distribution and verification of digital certificates.
PSIRT	**Product Security Incident Response Team** The PSIRT is responsible for vulnerability management at product level; see also CSIRT at system level.
RED / RED-DA	**Radio Equipment Directive (Delegated Act)** EU directive; the RED applies to devices with radio functionality, while the DA extension applies to security functions.
SBOM	**Software Bill of Material** An SBOM documents which commercial and free software components are contained in software products. It makes dependencies on third-party components transparent and thus helps to monitor vulnerabilities.
SIEM	**Security Information and Event Management** SIEM combines both SIM (Security Information Management) and SEM (Security Event Management) in one security management system. SIEM technology collects event log data from various sources, detects anomalous activities through real-time analysis and initiates appropriate countermeasures.
SL	**Security Level** The security levels defined in IEC 62443 describe the security requirements for an IT infrastructure. SL 0: No special requirements or protective measures SL 1: Protection against unintended or accidental misuse SL 2: Protection against intentional misuse using simple means with limited resources, general skills and low motivation SL 3: Protection against intentional misuse using sophisticated means, moderate resources, IACS-specific knowledge and moderate motivation; see also IACS SL 4: Protection against intentional misuse using elaborate means, extensive resources, IACS-specific knowledge and high motivation; see also IACS
SPDL	**Secure Product Development Lifecycle** Process description from IEC 62443-4-1 for a secure product development life cycle
VPN	**Virtual Private Network** VPN refers to a virtual private (self-contained) communication network. Virtual means that it is not a separate physical connection, but an existing communication network used as a transport medium. VPN is used to connect participants in the existing communication network to another network.
Zone	Network zones divide a system into homogeneous segments by grouping logical or physical systems with common security requirements. The security requirements of each zone are defined by means of security levels (SL).

Legal Notice: Weidmüller Interface GmbH & Co. KG, Klingenbergstraße 26, 32756 Detmold, Germany, Tel.: +49 5231 14280, Email: weidmueller@weidmueller.de, www.weidmueller.de | Limited partnership, Registered office: Detmold, Lemgo Local Court HRA 2790 | General partner: Weidmüller Interface Führungsgesellschaft mbH, Registered office: Detmold, Lemgo Local Court HRA 3924, VAT no.: DE124599660Managing Directors: Dr Sebastian Durst, Dr Timo Berger, André Sombecki, Dr Christian von Toll

Weidmüller – Your partner in Smart Industrial Connectivity

As experienced experts, we support our customers and partners around the world with products, solutions and services in the industrial environment of power, signals and data. We are at home in their industries and markets and we understand the technological challenges of tomorrow. That is why we are always developing innovative, sustainable and value-creating solutions for their individual needs. Together, we set new standards in Industrial Connectivity.

We cannot exclude the possibility of errors in our printed materials or in software that is provided to the customer for ordering purposes. We make every effort to correct such errors once we become aware of them.

Our general delivery conditions, which are available on our group website where you submit your order, apply to all orders. We are also happy to send these conditions to you upon request.

Made in Germany

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
Tel. +49 5231 14-0
Fax +49 5231 14-292083
www.weidmueller.de

Version 01/05.2026