Industrial Product Security Guideline

System overview with best practice

Weidmüller

Table of contents

Warning and Disclaimer

Warning
Devices may fail in unsafe operating conditions, causing uncontrolled operation. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer
This Guideline does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Guideline, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

Note
The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. This Guideline is not binding and does not claim to be complete in terms of configuration as well as any contingencies. By using this Guideline, you acknowledge that we cannot be held liable for any damages beyond the described liability regime.
We reserve the right to make changes to this Guideline at any time without notice. In case of discrepancies between the proposals in the Guideline and other Weidmüller publications, like manuals, such contents have always more priority than the Guideline. We assume no liability for the information contained in this document.
Our liability, for whatever legal reason, for damages caused by using the examples, instructions, programs, project planning and performance data, etc. described in this Guideline is excluded.

Security notes
To protect equipment, systems, machines and networks against cyber threats, it is necessary to implement and maintain a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorised access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards, such as firewalls and network segmentation, have been used.

1. Introduction

The rapid digitalisation and networking of industrial processes have transformed operational and automation technology (OT). While these advancements offer significant benefits - such as increased efficiency, flexibility, and productivity - they also introduce serious challenges, with cybersecurity being one of the most urgent. Cyberattacks on industrial systems are becoming more frequent, and a successful attack can lead to devastating consequences, including production downtime, environmental harm, or even loss of life.

As industrial systems grow more complex and interconnected, traditional security measures are no longer enough. Hackers and other malicious actors are actively seeking vulnerabilities in OT networks to exploit for disruption or data theft. It is essential that organisations in the OT sector take proactive steps to protect their systems against these threats.

In response to these challenges, regulatory bodies in the EU have introduced a series of cybersecurity laws and directives that place new requirements on companies and products. Weidmüller supports these initiatives by offering a range of solutions designed to enhance the security of your machines and systems.

This document provides guidance on how to establish a robust cybersecurity system and how to integrate Weidmüller components within that system. Consequently, the document repeatedly refers to the international IEC 62443 standard, which was developed to address the cybersecurity needs of industrial automation systems. This standard offers a comprehensive framework for planning, implementing, and maintaining security measures in OT networks.

Weidmüller has certified its safe product development process according to IEC 62443-4-1 and will also introduce IEC 62443-4-2 compliant products.

In addition to this overview, detailed security documents for specific product groups are also available. These documents provide quick access to security functions that can be used for planning or conducting security risk analyses. You can find product-specific security documents in our **eShop** or in the **Weidmüller Support Center**. Please search for your specific product.

www.weidmueller.com/eshop

www.weidmueller.com/support-center

Note: Technical information on the secure use and operation of our products is available in the "Defense-in-depth" chapter.

1.1 Difference between IT and OT

Information Technology (IT) and Operational Technology (OT) are two key areas within industrial companies. While they are often interconnected and complement each other, they serve different purposes and face different challenges.

IT (Information Technology) deals with the processing, storage, and transmission of data. It supports business processes and administrative tasks through systems like computer networks, databases, and software applications. In IT, security is primarily focused on protecting data from unauthorised access, theft, or manipulation. The priorities in IT security are:

- Confidentiality
- Integrity
- Availability

OT (Operational Technology) involves the control, monitoring, and automation of physical processes and machinery in industrial environments. This includes devices like sensors, actuators, industrial control systems, and robots. In OT, the focus is on ensuring the continuous operation and security of systems and infrastructure. OT environments require specialised security solutions beyond those used in IT.

The security priorities in OT are:

Figure 1: OT security priority

1.2 Difference between Security and Safety

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

Safety, in contrast, focuses on protecting people, the environment, and physical resources from hazards and accidents. It aims to ensure the physical well-being of employees, prevent injuries, and avoid industrial disasters or environmental harm.

Both, security and safety, are essential for ensuring the overall integrity and reliability of systems. Achieving safety will be impossible without addressing security as well.

2. Security laws and Standards

Until recently, security laws primarily focused on critical infrastructure. Due to the increasing threat of cyberattacks, new regulations are expanding cybersecurity requirements for companies and products across various industries.

Law	Region	Target group	Comments
NIS (Network Information System Security) EU 2016/1148	EU	Asset Owner, Plant operators of critical infrastructure	Requires the implementation of a cybersecurity management system. Enforced through national laws in EU countries.
Cybersecurity and Infrastructure Security Agency Act	USA	Asset Owner, Plant operators of critical infrastructure	Requires the implementation of a cybersecurity management system for critical infrastructure.

2.1 New and Expanded Security Laws

As cyber threats pose increasing economic risks, security requirements for businesses and products are being significantly expanded. The EU, in particular, is introducing new or extended laws with cybersecurity provisions.

Law	Mandatory from	Target group	Comments
NIS2 (Network Information System Security) EU 2022/2555	EU target Oct. 2024	Asset Owner, Plant operators	Expands the NIS scope to include more industrial sectors (e.g., machinery, electrical industries) and smaller companies (>50 employees, >€10 million turnover). Implementation into national law necessary.
RED DA (Radio Equipment Directive – Delegated Act) EU 2033/30	Aug. 2025	Device / Machine manufactures	CE marking requirement for devices with wireless interfaces that can communicate directly or indirectly with the internet.
Machinery Regulation EU 2023/1230	Jan. 2027	Machine manufactures	CE marking requirement for machines. New security requirements.
CRA (Cyber Resilience Act) EU 2024/2847	Dec. 2027	Device / Machine manufactures	CE marking requirement for devices or software with digital elements and data communication.

2.2 Industry-Specific Security Standards

Certain organisations have introduced cybersecurity requirements for specific industry sectors.

Standards from organizations	Mandatory from	Target group	Comments
IACS UR-E26/27	July 2024	Ship Owner, Ship operators.	International Association of Classification Societies (IACS) standards requiring cybersecurity systems for new ships.

2.3 International Security Standards

Cybersecurity extends beyond securing individual components; it requires a holistic approach to protect systems, networks, data, and infrastructures across multiple layers. A comprehensive security management system (CSMS) must be in place, defining requirements for the establishment, implementation, maintenance, and continuous improvement of cybersecurity measures. Below are key international standards relevant to cybersecurity.

Standard	Focus	Target group	Comments
ISO / IEC 27001	IT	Asset Owner, Plant operators	Defines an Information Security Management System (ISMS) with a focus on IT security.
ISA / IEC 62443	OT + IT	Asset Owner, Plant operators, Device manufacturer	Defines a Cybersecurity Management System (CSMS) for OT and IT, covering requirements for operators, system integrators, and component manufacturers.

2.3.1 Standard IEC 62443

The IEC 62443 standard is a series of international standards and technical reports developed specifically for the cyber security of industrial automation systems. The standard was developed by the International Electrotechnical Commission (IEC) in order to address the specific requirements and challenges of OT systems and provide clear guidelines for the implementation of security controls and procedures in industrial environments.

The standard covers the following aspects:

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

Each part is designed to guide different stakeholders, such as plant operators, system integrators, and component manufacturers. For example, IEC 62443-2-1 provides a mapping to ISO 27001, focusing on IT security, allowing a comprehensive approach to OT security. IEC 62443 can therefore be used comprehensively for OT security.

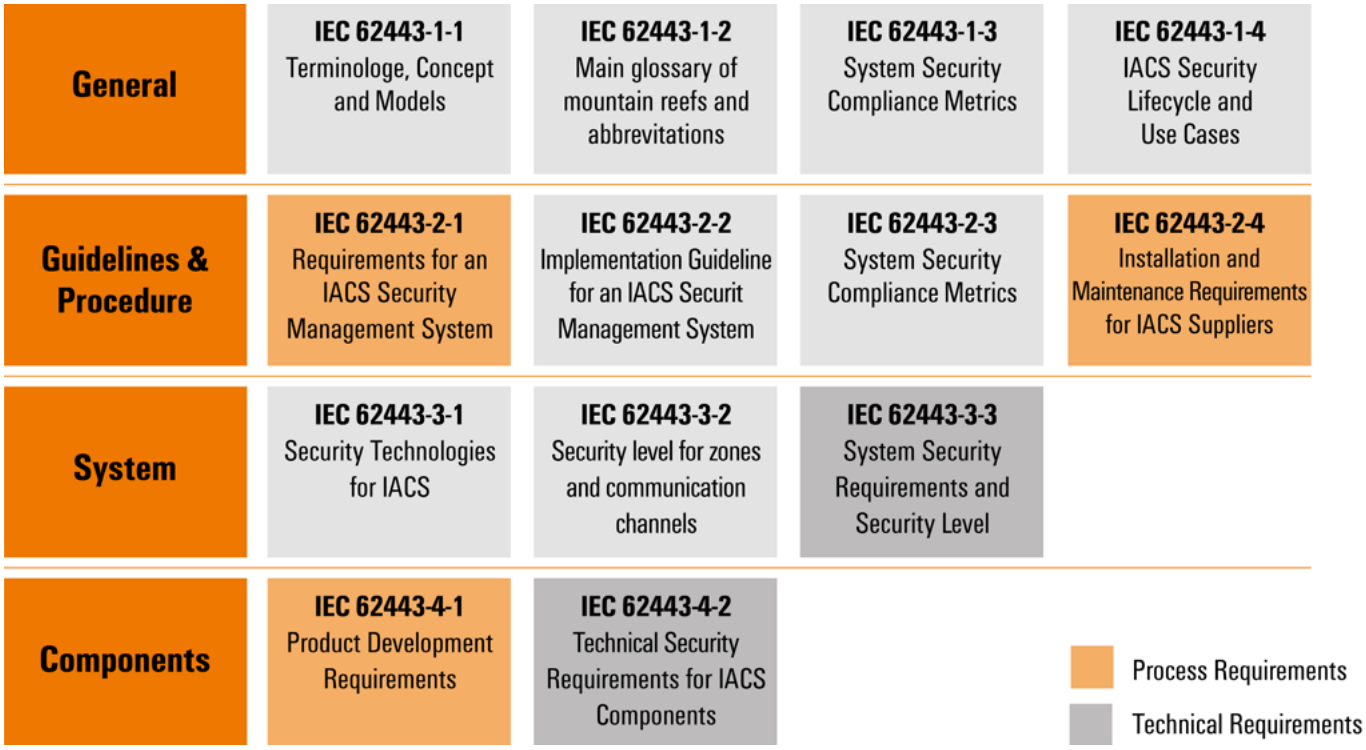

Figure 2: Parts of the IEC 62443

The Cyber Security Management System (CSMS) of IEC 62443 is based on the following core elements:

Business rationale
Business rationale is to clarify which business elements are to be protected and how important they are for the business in case of a successful cyberattack. This includes financial issues as well as safety, health, environmental and reputational aspects.

Risk identification, classification and assessment
Identifying the set of cyber risks that an organisation faces and assessing the likelihood and severity of these risks.

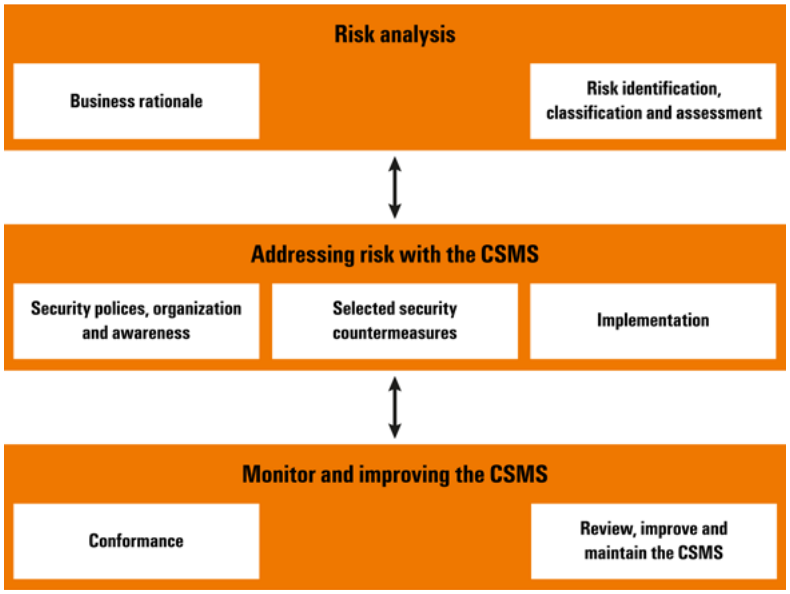

Figure 3: Cyber Security Management System (CSMS)

Security polices, organization and awareness
This part addresses strategic and organization topics like:

- Scope of the security management system
- Organising for security
- Staff training and security awareness
- Business continuity plan
- Security policies and procedures

Selected security countermeasures
Defining security controls at minimum for the main elements:

- Personnel security
- Physical and environmental security
- Network segmentation
- Access control

Implementation: Implementing measures to mitigate risks and achieve security objectives.

Conformance: Ensure that the CSMS developed for an organisation is followed.

Review, improve and maintain the CSMS: Ensure that the CSMS continues to meet its goals over time.

Weidmüller Compliance

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

2.4 North American Cybersecurity Guidelines for OT Environments

2.4.1 Cyber Resilience Act (CRA)

While the CRA is primarily an EU initiative, North American organisations must also consider its implications, especially if they manufacture or supply products to European markets. The CRA focuses on ensuring the **cybersecurity of digital products** throughout their lifecycle, including secure development, deployment, and maintenance.

2.4.2 Key Aspects for North America

- **Product Compliance:** Manufacturers must ensure that their OT systems are secure-by-design and support secure updates.
- **Digital Elements:** Any OT products or software with digital communication elements (e.g. Industrial IoT devices) should meet the security standards outlined in the CRA.

2.4.2.1 Key Layers for North American Organisations:

- **Cybersecurity Management System (CSMS):** Establish a structured cybersecurity management process.
- **Network Segmentation:** Use zones and conduits to limit security risks (e.g. secure zones for critical processes).
- **Device Security:** Manufacturers must follow secure-by-design principles for devices and components used in OT environments.

2.4.3 ISA/IEC 62443 for OT Security

ISA/IEC 62443 is a comprehensive standard for cybersecurity in industrial automation and control systems. It provides a framework to secure OT environments, from plant operators to component manufacturers.

2.4.4 NIST Standards (NIST 2.0)

The **National Institute of Standards and Technology (NIST)** provides a cybersecurity framework widely adopted across North American industries, including critical infrastructure and OT environments. The latest version, NIST 2.0, focuses on proactive security measures and improving cyber resilience.

2.4.4.1 NIST 2.0 Key Elements for OT

- **Identify:** Understand and catalog OT assets and risks.
- **Protect:** Implement safeguards 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 disaster recovery and business continuity plans are in place.

2.4.4.2 Comparative Table

Standard	Focus	Applicable Areas
CRA	Digital product lifecycle security	Manufacturers of OT devices and software
ISA / IEC 62443	Cybersecurity for OT environments	Asset owners, integrators, and component manufacturers
NST 2.0	Comprehensive cybersecurity framework	Asset owners and critical infrastructure providers

3. Defense-in-depth

The "Defense-in-depth" security concept is a strategic approach with the aim to protect systems and networks from a variety of threats by implementing multiple layers of security. The idea behind this concept is that a single security measure is not enough to fully protect a system. Instead, multiple layers or layers of security are implemented to detect, prevent, or mitigate potential attacks at different levels.

Defense-in-depth is a multifaceted strategy that integrates people, technology, and operational capabilities to establish variable barriers across multiple layers and dimensions of the organisation.

There are various layers:

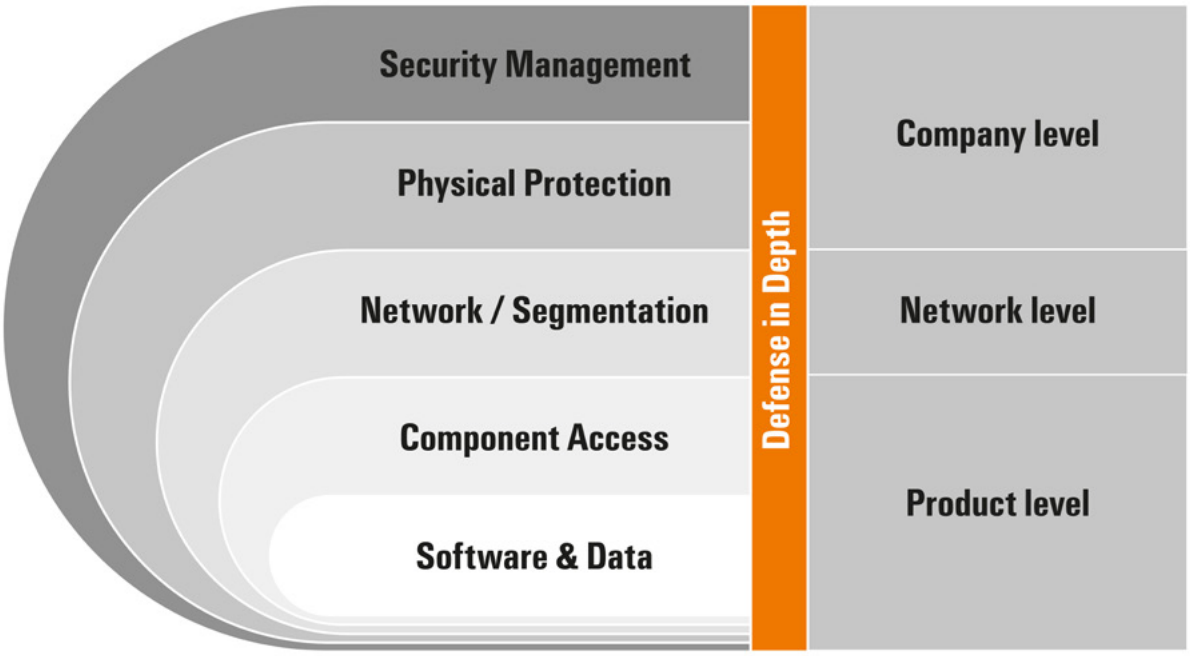

Figure 4: Layer model "Defense-in-depth"

The following sections describe the individual layers and how Weidmüller components can support you in setting up a security system.

3.1 Defense-in-depth Layer: Security Management

Security management is a higher level cybersecurity program that supports the security protection of the OT environment. This layer references as specially to organisational topics by setting up a cybersecurity management system (see above chapter ‘Standard IEC 62443’ as an example). This includes policies, processes, and awareness. These programmatic and organisational decisions will guide and impact the decisions needed for the other defense-in-depth layers.

Typical topics in this layer are:

- Awareness and training of personnel
- Definition/review of responsibilities of plant users
- Definition/review of user roles
- Definition/review of user access rights
- Regulations of physical access
- Implementation of an incident response plan
- Definition of a patch management system for rolling out security patches

3.1.1 PSIRT

PSIRT stands for "Product Security Incident Response Team". The PSIRT is a specialised team within a company or organisation that deals with the resolution of security incidents in products or software. When security gaps or vulnerabilities are discovered in a product, the PSIRT is responsible for investigating, assessing, and remediating them. In addition, a PSIRT communicates with customers, suppliers, and other relevant parties to disseminate information about security issues and offer solutions.

Weidmüller has established a PSIRT and provides information on product-specific security vulnerabilities and their elimination on the **Weidmüller website**.

www.weidmueller.com/security-advisory-board

In addition, Weidmüller publishes security vulnerabilities of its products at **CERT@VDE**. CERT@VDE is a neutral, non-profit platform. The CERT@VDE supports its partners in questions of cybersecurity in products of the automation industry in order to facilitate fast, structured and professional handling of security gaps.

www.cert.vde.com/en

3.1.2 CSIRT

CSIRT stands for "Computer Security Incident Response Team". In contrast to a PSIRT, a CSIRT focuses not only on products, but also on the general IT infrastructure of an organisation. A CSIRT is responsible for detecting, responding, and managing security incidents in a broader context.

3.2 Defense-in-depth Layer: Physical Protection

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

- Examples of a physical access control
- In general, minimise the group of people with access authorisation.
- Secure your cabinet doors with improved access protection, e.g. with keys.
- Secure service interfaces that are accessible from the outside of the cabinet, for example with the lockable FrontCom Vario system from Weidmüller.

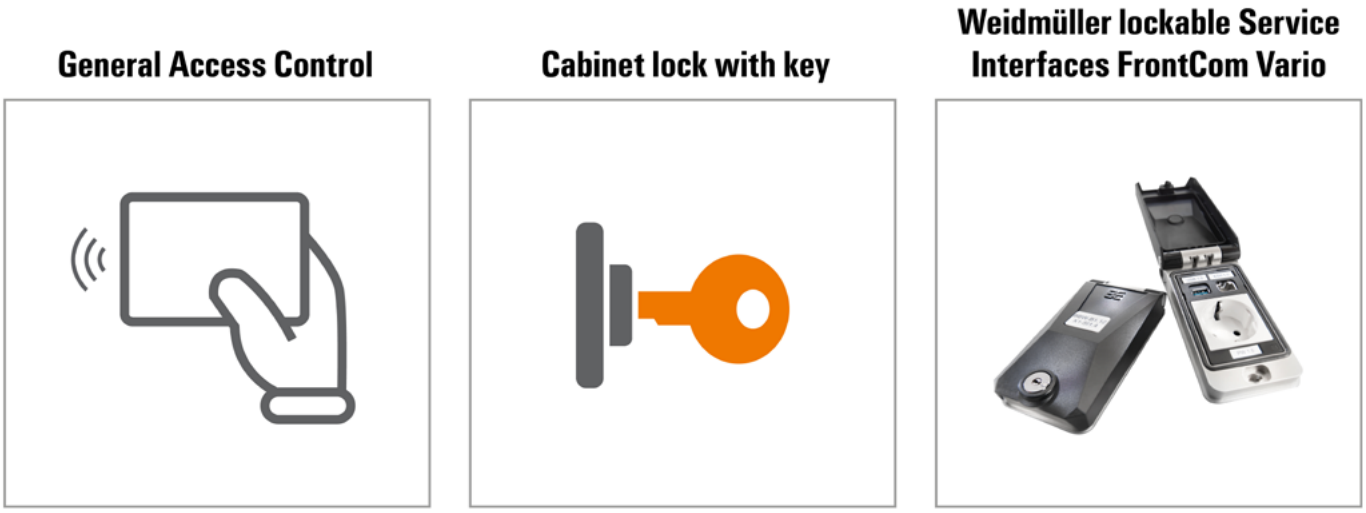

Figure 5: Examples of physical access systems

Note:
The 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 should only be permitted to authorised persons.

3.3 Defense-in-depth Layer: Network / Segmentation

The network is a major target for cyberattacks. An essential countermeasure is network segmentation to minimise a possible attack to a limited area.

Basic principles for network segmentation (zones and conduits)

a. Avoid large zones: Large zones can create vulnerabilities. Keeping zones small helps contain potential threats.
b. Define hierarchical zones: Establish zones at the same security level to simplify management and enhance security.
c. Secure transitions (conduits): Ensure that transitions between zones are well-protected. Use firewalls to restrict communication to only what is necessary.

A network architecture with zones and conduits is shown here as an example.

Zone: yellow coloured segment. A group of components with the same target-level.

Conduit: orange coloured line. 'Protected' channel to exchange data.

Typically, the router protects the zones and rules out the allowed conduits with the firewall to allow only necessary communication. Communication in a conduit should be encrypted wherever possible. If this is not provided by the used protocol, a secure channel (via VPN tunnel) or secure encrypted communication, e.g. HTTPS, OPC-UA,.

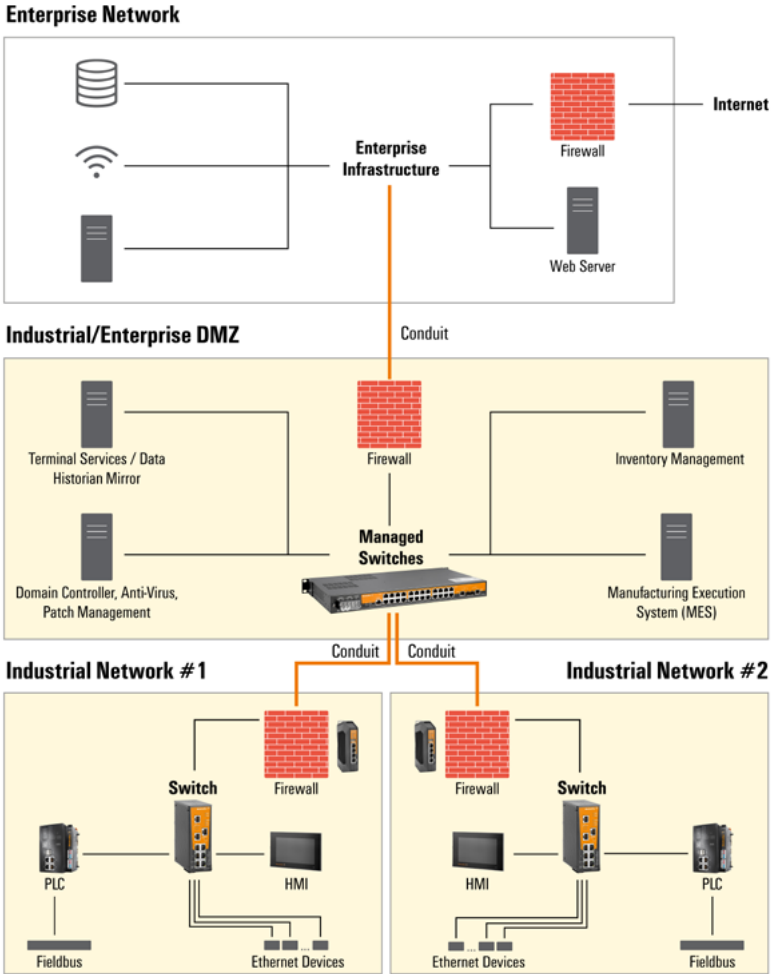

Figure 6: Concept zones and conduits

There are various system concepts for zones and conduits as shown in the picture. A company must decide on the optimum architecture individually, although the basic principles are identical.

The DMZ stands for Demilitarized Zone and refers to a specially controlled network that is located between the external network (Internet) and the internal network or between two critical internal networks. It is a kind of buffer zone that separates the networks from each other by means of strict communication rules and firewalls.

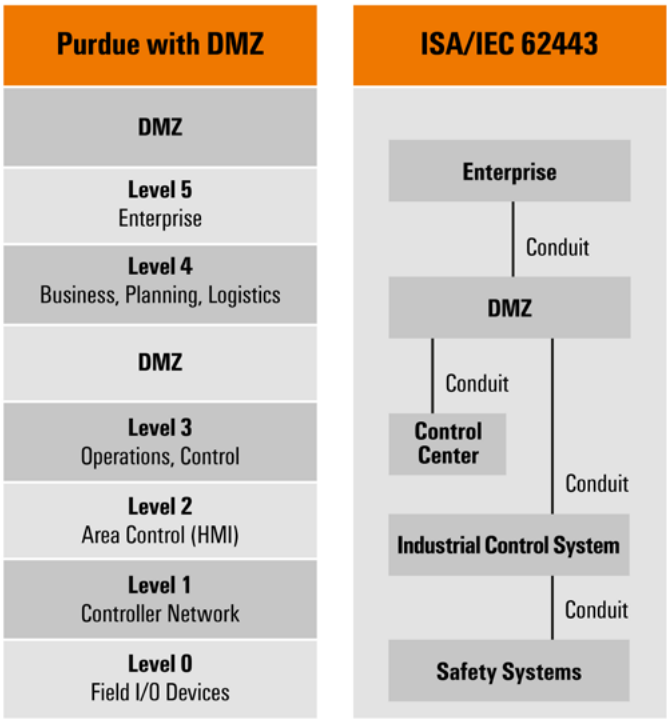

Figure 7: Different zone concepts

The following is an example of the automation structure of a machine and the OT network infrastructure of the factory floor with Weidmüller components.

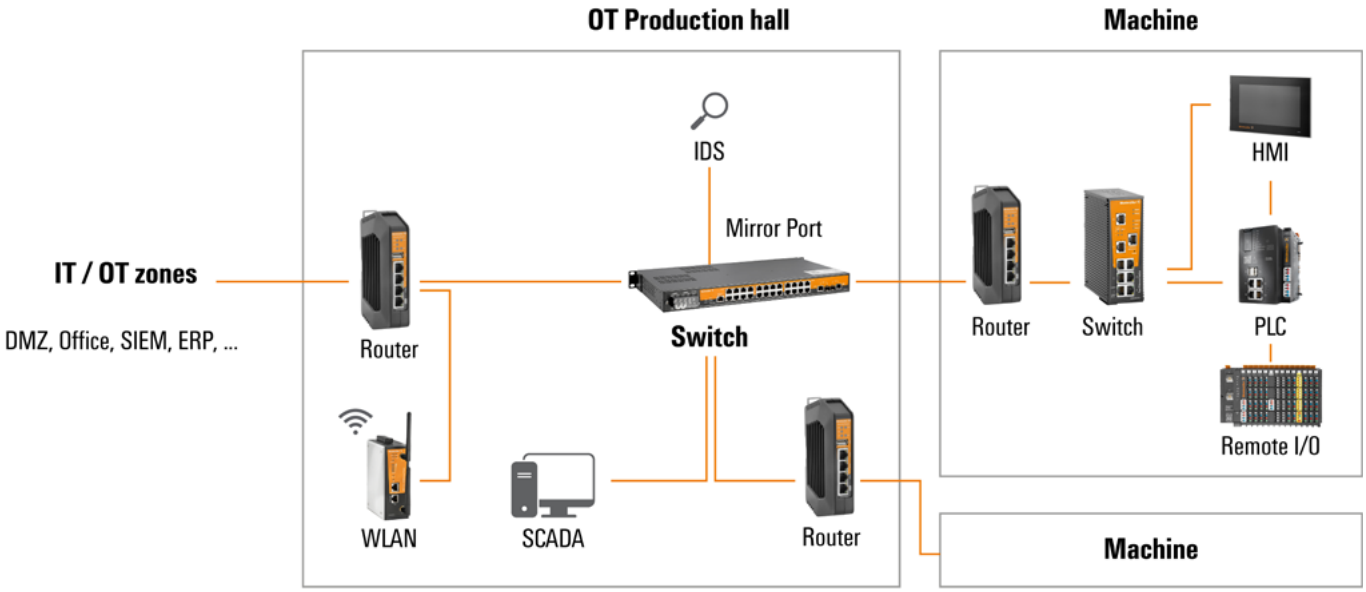

Figure 8: Example network segmentation structure.

Weidmüller Compliance

- **Segment Networks:** Segment the network into zones with the same security level. Create zones within machines and the OT shop floor using Routers, VLANs or Layer 3 switches.
- **Use Firewalls:** Secure machines with routers equipped with firewalls, either integrated or positioned externally.
- **Protect Fieldbus Networks:** Implement physical access controls for fieldbus segments due to their lower security level.
- **Isolate Wi-Fi Networks:** Use separate VLANs for Wi-Fi access, accompanied by robust security measures like firewall rules and centralized access management (e.g. IEEE 802.1X).
- **Consider Intrusion Detection Systems (IDS):** Deploy IDS to monitor for attacks, using managed switch mirror ports to analyse traffic.

The following concepts support network segmentation security.

3.3.1 Switches and VLAN

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

Traditionally, devices in a network are segmented by physical connections. VLANs, on the other hand, make it possible to group devices in a network based on logical criteria such as function, department, application, or security criticality regardless of their physical position in the network. This segmentation offers more flexibility, security, and efficient use of resources

Weidmüller managed switches offer port based VLAN (Virtual Local Area Network) and tagged VLAN support, allowing for logical segmentation of the network. This makes it easy to set up network segments with different security levels in the machine, in the production line or the plant.

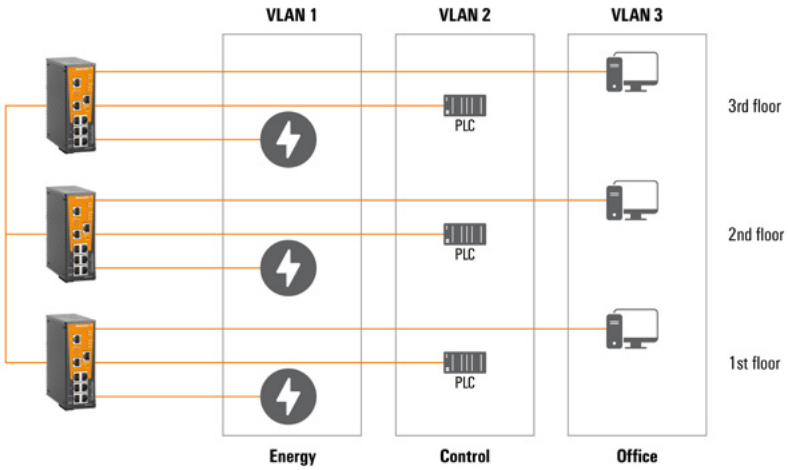

Figure 9: VLAN Segmentation

Weidmüller managed switches offer port based VLAN (Virtual Local Area Network) and tagged VLAN support, allowing for logical segmentation of the network. This makes it easy to set up network segments with different security levels in the machine, in the production line or the plant.

You can also use Weidmueller Ethernet switches in conjunction with fieldbus systems such as PROFINET or EtherNet/IP. Please refer to the technical data of the switches.

More information about security on Fieldbus see chapter “3.3.3 Fieldbus ”.

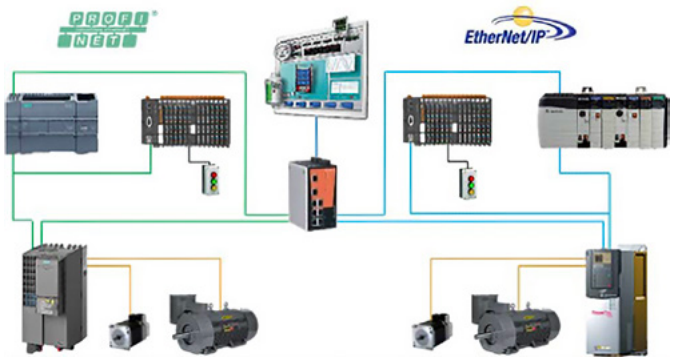

Figure 10: Fieldbus network with switch

Best Security Practices for Switches

- **Implement VLANs:** Use VLANs to segment networks by security criticality (e.g. separate Wi-Fi access points or Energy Meter).
- **Secure Management Interfaces:** Disable HTTP and use HTTPS for web interfaces. Disable TELNET in favor of SSH for CLI access. Optionally set the management VLAN ID of the switch to a separate VLAN so that the web interface of the switch can only be reached via a separated VLAN (e.g. only one port in the network system).
- **Limit SNMP Use:** Disable SNMP if not used. If necessary, use SNMPv3 with a strong password.
- **Deactivate Unused Services:** Turn off any unnecessary services (e.g. PROFINET,...) to reduce potential attack vectors.
- **Lock Down Unused Ports:** Use port lock features to deactivate unused physical ports.
- **Static MAC Address Binding:** Use MAC or IP address bindings to restrict network access.
- **User Profile Management:** Create multiple user profiles with specific rights based on roles.
- **Configure Access Control Lists (ACLs):** Implement ACLs to control network traffic if useful.

3.3.2 Routers

Network routers are critical components for network security as they can control, segment and filter traffic to minimise potential threats and ensure the protection of sensitive resources. Typically, they are the endpoints of conduits.

Routers have the following typical functions:

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

Firewall functionality: Modern routers have built-in firewall functions that can monitor and filter incoming and outgoing traffic. These firewalls can help block unwanted traffic, detect and prevent potentially harmful activity and improve data protection 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 data in the superimposed network (or Internet). This provides a degree of security by protecting the internal network addresses from direct disclosure to external networks. This can help reduce the attack surface and protect the privacy of internal network resources.

VPN (Virtual Private Network): Routers can provide VPN functionality to establish secure connections between remote sites or users. VPNs encrypt traffic and provide secure communication over insecure networks such as the Internet. This allows remote users to securely access company resources without compromising security.

Best Security Practices for Routers

- As an overview, please watch the **video tutorial** on the secure configuration of a router.

  www.weidmueller.com/secure-router-configuration

- **Change the Firewall (Packet Filter) settings:** Weidmueller Industrial Security Routers have a performant whitelisting firewall. That means all communication that does not match to a rule top-bottom principle will be dropped. The routers contain one firewall rule by factory default: “Allow All”. To improve security, make a list of communication which flows via the router. Then add these communication parameters to the Firewall setting for a whitelisting. When all required traffic is listed, delete the rule “Allow All” to ensure that other traffic will be blocked.
- **Perform access restrictions:** Weidmueller Industrial Security Routers offers the possibility to create various user profiles which can obtain rights on a granular level.
- Only grant access to the persons who need access with only those rights that are needed for their tasks.
- **Secure Management Interfaces:** Deactivate HTTP access of the router on all interfaces.
- **Access via public network:** Deactivate HTTPS access of the router on interfaces that are exposed to a public network (WAN / Mobil WWLAN) if not necessary. Use VPN to communicate with public network.
- **Limit SNMP Use:** SNMP is deactivated by default. If you use it, please make sure to use SNMP v3 and choose a strong password instead of default.
- **Use VPN for unsecure network:** For accessing your local network segment remotely (via an unsecure network), a Virtual Private Network (VPN) is recommended.
  With Weidmueller Security Router this can be done using an open technology as OpenVPN or IPsec or the Weidmüller u-link Remote Access Service.
- **Use NAT for unsecure network:** In case the Router is connected directly to a public network (e.g. via 4G), activate NAT masquerading on the interfaces to hide local IP addresses.
- More information in chapter ‘Remote Access”

3.3.3 Fieldbus Network

Fieldbuses such as PROFINET, EtherNet/IP, EtherCAT, Powerlink, CANopen or Modbus are optimised for low cycle times with low jitter and data consistency with regard to their real-time communication. Encrypted data transmission is not given with this real-time transmission. Furthermore, 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 often used for engineering the controller and fieldbus configuration as well as for the controller-independent configuration of fieldbus devices. The device can be accessed 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 the user management (see chapter 3.4 Defense-in-depth Layer: Component Access).

According to the current state of the art, we recommend separating the control and system network from other networks within an operational network infrastructure. We also recommend strict access control to such machine and system parts.

Best Security Practices for Routers

- **Restrict Physical Access:** Secure access to fieldbus networks with physical access controls.
- **Separate Networks:** Separate the fieldbus network from other networks.
- **Make Small Segments**: Segment large fieldbus networks to smaller once to limit a possible cyberattack to a smaller area.
- **Secure Transitions:** Communication transitions to other zones should be secured by routers with appropriately configured firewall rules.
- **Use Fixed IP Addresses:** Assign fixed IP addresses to the devices and avoid the use of DHCP services.
- **Use HTTPS:** Use secure HTTPS communication instead of HTTP.
- **Deactivate Web Server Access via Fieldbus:** To minimise cyberattack possibilities, some u-remote fieldbus couplers offer the option of prohibiting web server access via the fieldbus. Web server access is then only possible via USB. If possible, deactivate fieldbus web server access.
- **Check Fieldbus documentation:** Observe the fieldbus-specific documentation to ensure the secure possible operation.

3.3.4 Remote Access Service

Remote access allows users to connect to a network or device from a remote location, typically via a Virtual Private Network (VPN). While it enhances productivity by enabling work from various locations, it can also introduce security vulnerabilities if not properly secured.

Key considerations:

- Security risks: Remote access can provide attackers with opportunities to gain unauthorised access to sensitive systems and data. Therefore, implementing robust security measures is essential.
- Collaboration: Establish a clear agreement between the machine manufacturer and the operator regarding the scope of remote access. On-site personnel should be present for critical activities, with local approval required for access.

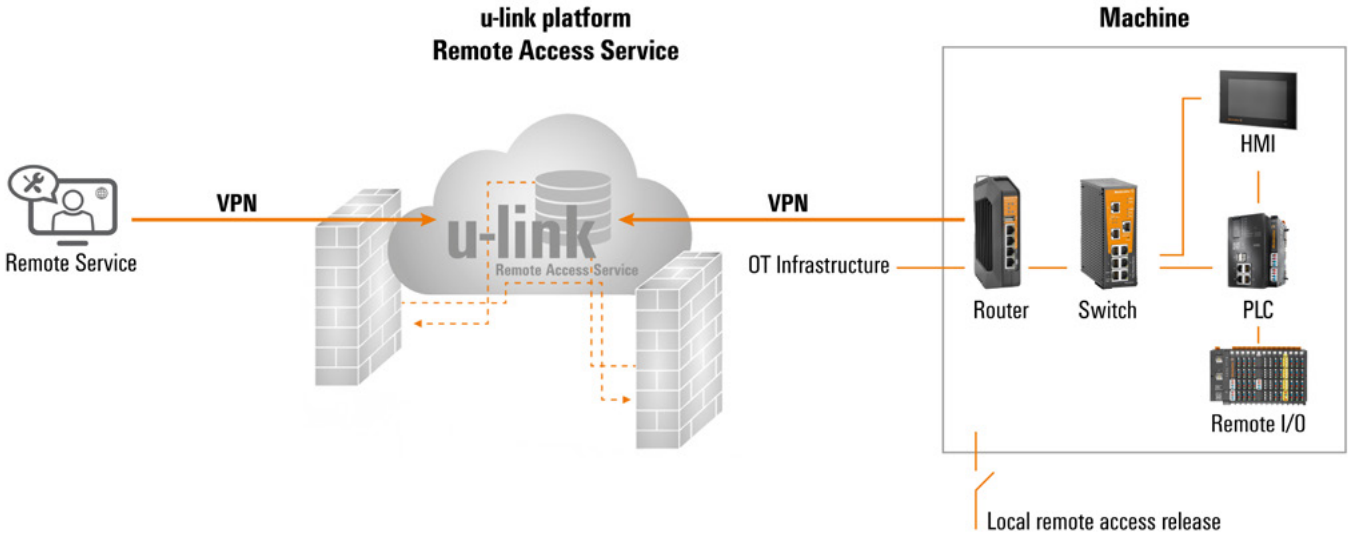

Figure 11: Remote Access Service with u-link

Weidmüller u-link System
With u-link, Weidmüller provides a secure remote access solution including:

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

The u-link platform adheres to ISO 27001 standards and features robust security functionalities, including:

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

Best Security Practices for Routers

- **Use Secure VPNs:** Implement a securely encrypted VPN connection, such as the Weidmüller u-link, to protect data during remote access.
- I**mplement Multi-Factor Authentication (MFA):** Enforce MFA to enhance the security of remote access services. U-link offers options for MFA.
- **Apply Least Privilege Principle:** Configure user rights so that individuals have only the necessary permissions for their task. This includes specifying which devices and ports can be accessed.
- **Pre-Agreement on Remote Access Scope:** Establish a clear remote access agreement between the machine manufacturer and the operator before any access is granted.
- **Local Authorization for Remote Access:** Use physical switches or similar methods to grant or deny remote access. Weidmüller u-link routers feature a digital input to control remote access based on local approval.
- **Prepare Systems for Software Updates:** Ensure that the machine or system is in a safe state before transferring and installing software updates to minimize risks.

3.4 Defense-in-depth Layer: Component Access

At Weidmüller, information access to a device is referred as User Management. Alternatively, the following terms are commonly used:

- Access management
- IAM (Identity and Access Management)
- User & Permission Management

User Management has the following core elements:

- **Identification:** Establishing a unique identity for each user within the system (e.g. usernames).
- **Authentication:** Verifying the identity of users (e.g. through passwords or other verification methods).
- **Authorisation:** Defining what actions and resources an authenticated user can access (e.g. permissions for configuration changes).

All Weidmüller devices with a web browser interface have a user management system to protect against unauthorised changes.
The authorisations can be specified very granularly depending on the device.
User management is a decisive element for security protection and should be used conscientiously in accordance with the security requirements.

3.4.1 Strong Password

Recommended is a password strength of at least 8 signs including small and capital letters, numbers, and special characters.
We recommend to use 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.

Note: u-remote requires 3 different character types.

3.4.2 Least Privilege Principle

The least privilege concept is a fundamental security principle, which states that users should only be given the minimum permissions they need to perform their respective tasks. In other words, a user should only be granted the access rights that are absolutely necessary to do their job and nothing beyond that. This concept serves to minimise the security risk by reducing potential attack surfaces.

In practice, the least privilege concept means that administrators should carefully review access rights and grant only those permissions that are necessary to perform a user's tasks. This requires a thorough analysis of roles and responsibilities within the organisation as well as regular review and adjustment of permissions to ensure they are up to date and appropriate.

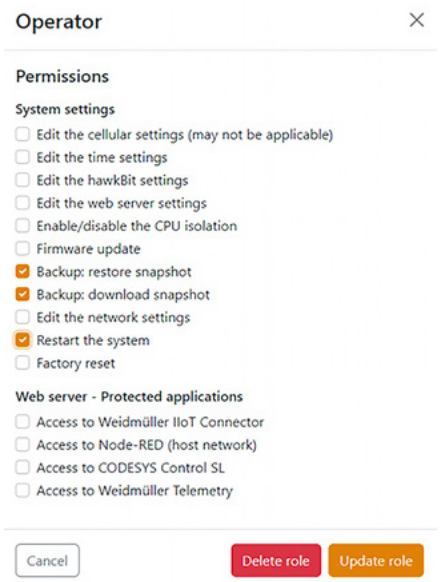

Figure 12: Access rights definition in u-OS

3.4.3 Browser message 'Insecure connection' or 'Your connection is not private'

When connecting your web browser to the Weidmüller device, you often receive the browser message 'insecure connection', 'Your connection is not private' or similar. This is due to the security settings of your browser or the self-signed certificate on the device.

Here is an example from a Chrome browser.

The reason for using Weidmüller self-signed certificates is that a certificate is linked to the IP address used. As this address is typically customised to the application, the user must also issue a customised certificate. Further information can be found in the following chapter.

To communicate with the Weidmüller device, please click on 'Advanced' or similar and select that you want to communicate with the device insecurely

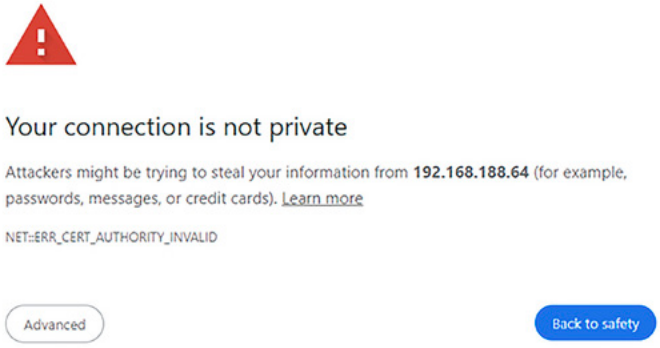

Figure 13: Possible browser message

3.4.4 Creating and exchanging certificates

A certificate enables a secure communication connection with HTTPS. The green lock symbol in the browser indicates that this website has a valid and trustworthy certificate, and that the connection is secure.

It is recommended to replace the existing Weidmüller certificates with your own certificates.

If possible, specially created certificates should be signed by a certification authority (so-called 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.

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.

Please select the key type RSA and the key size of 4096 bit.

You can find a **video tutorial** for creating self-signed certificates in the Weidmüller Support Center

www.weidmueller.com/creating-certificates

Best Security Practices for Routers

- **Use HTTPS Certificate:** Create your own certificate for HTTPS communication (see chapter above).
- **Apply Least Privilege Principle:** Use the least privilege concept described in chapter “3.4.2 Least Privilege Principle”.
- **Change Password:** Change the default password during initial configuration of the device.
- **Use a Strong Password:** Please use a strong password see chapter “ 3.4.1 Strong Password”.
- **Use Unique Passwords:** Don’t use one password for several applications.
- **Use Individual Passwords:** Recommended is a unique identifier (free choice name) for every user.
- **Secure Management Interfaces:** Activate HTTPS (deactivate HTTP) access of the device for interfaces with user interactions.

3.5 Defense-in-depth Layer: Software & Data

This Defense-in-depth layer covers security topics that are located in a device and essentially deal with the handling of software and data.

This includes:

- Firmware and their updates
- Apps and their updates
- Applications
- Backup and Restore
- Logging

3.5.1 Firmware and updates

Weidmüller uses specially industrially hardened operating systems in its devices and offers software updates for its products. Please check our **Support Center** periodically to see if 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.
In the case of Weidmüller security routers, new firmware can also be easily installed on the connected routers using 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 directly or on a scheduled basis.

For devices with the u-OS operating system, Weidmüller also offers an automated update function, known as rollout management, in addition to manual updates via the web user interface. The rollout management is integrated into the Weidmüller easyConnect platform. The open source software Hawkbit is used for this. This also enables alternative server operation directly in the company network.

Best Security Practices for Firmware and updates

- **Use Secure Sources:** Make sure that you only download updates from trustworthy sources, e.g. Weidmüller Support Center
- **Check for Updates:** Check cyclically for new updates for the devices you are using.
- **Install Security Updates in a Timely Manner:** Install software updates and security fixes as quick as possible.
- **Updates only in Safe Machine State:** Bring the machine or system into a safe state before the update.
- **Test Updates:** Test the new software before installing it on a large scale.
- **Service Personal present:** Make sure that service personnel are present at the machine or system during an automatic update so that they can react in the event of a safety incident.

3.5.2 Backup and Restore

Backup and restore are extremely important in the context of a security management systems because of:

- Data recovery after a security incident
  When a security incident such as a data loss, ransomware attack or system failure occurs, backups can be used to restore the affected data. This minimises the damage that such an incident can cause and allows companies to get back up and running quickly.
- Protection against data loss
  By making regular backups, companies can ensure that their 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 industries and legislation require organisations to create backups of their data and retain them for a certain period to ensure data integrity and availability.
- Protection against ransomware
  In the case of ransomware attacks, having backups can prevent an organisation from having to pay a ransom to restore their data. If they have up-to-date and intact backups, they can restore their data without having to give in to the attackers.
- Recoverability from human error
  People make mistakes, whether by accidentally deleting files or making unintentional changes to data. Backups provide a way to restore data to a previous state and correct human error.
- Business continuity
  Backups play an essential role in maintaining business continuity. If an unexpected event occurs that affects access to data, backups can be used to continue business operations while the problem is resolved.

Weidmüller devices supports Backup & Restore functionality. Please read the device-specific procedure in the device manual.

Best Security Practices for Backup & Restore

- **Regular Backups:** Carry out regular backups of your devices.
- **Safe Storage:** Keep the backups in a safe place.
- **Long Time Storage:** Keep backups for a longer period of time. The malware may have infected the system much earlier than the attack was detected.
- **Check recover process:** Check the recover function cyclically to ensure that the backup and recovery process is working.

3.5.3 Logging

Logging is an essential functionality in the 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 advantages:

- Event tracking:
  Logs provide a detailed record of events that occur on a system or network. These events can include attacks, unauthorised access, failed logon attempts and other suspicious activity. By analysing logs, security teams can identify and respond to potential security incidents.
- Forensic analysis:
  Logs are critical for forensic analysis of security incidents. They enable security analysts to reconstruct the course of an attack, identify affected systems and assess the extent of the damage.
- Compliance:
  Many security regulations and standards require logging of certain events and activities. By logging, organisations can ensure that they meet the requirements of compliance guidelines.
- Early detection of threats:
  By continuously monitoring logs, potential security threats can be detected early. Anomalies in the behavior of users, systems or applications can indicate potential security incidents that require further investigation.

- Auditing and tracking:
  Logs are also used to audit user activity and system operations. They allow organisations to understand who accessed which resources, what actions were performed and when they took place. This is important to ensure the integrity and confidentiality of data.

Weidmüller network components such as managed switches, security routers or Wi-Fi access points support the logging of security events.

Ideally, these security events should be made available to a higher-level system such as a SIEM. A SIEM (Security Information and Event Management) system is a software solution that is used to centrally monitor, analyse, and manage security events in real time. SIEM systems combine security information management (SIM) and security event management (SEM) and offer a comprehensive platform for security monitoring and response.

The Weidmüller network components use the SYSLOG protocol to forward security events to a SIEM system.

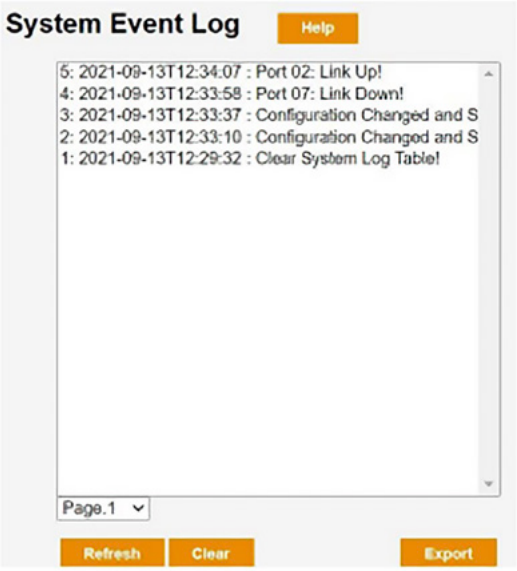

Figure 14: Event log example

Best Security Practices for Backup & Restore

- **Use Logging:** Use the logging functionality in your Weidmüller device (Eventlog, Event Log).
- **Interfacing 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 in general

3.5.4.1 APPs and updates

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

Weidmüller offers its own and 3rd party Docker containers as ready-made apps that can be loaded and executed on the device.

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

Best Security Practices for Backup & Restore

- **Use Secure Sources:** Make sure that you only download updates from trustworthy sources (e.g. Weidmüller APPHUB or Weidmüller Support Center)
- **Check for Updates:** Check cyclically for new updates for the devices you are using.
- **Install Security Updates in a Timely Manner:** Install software updates and security fixes as quick as possible.
- **Updates only in Safe Machine State:** Bring the machine or system into a safe state before the update.
- **Test Updates:** Test the new software before installing it on a large scale.
- **Service Personal present:** Make sure that service personnel are present at the machine or system during an automatic update so that they can react in the event of a safety 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 as well as real-time communication with various fieldbuses and communication to higher-level systems such as servers or cloud applications. This also includes PC-based engineering with the corresponding interfaces to the device and the CODESYS App.

This results in several security attack options, which are shown in the image.

CODESYS is a partner product from CODESYS Group. You can find further information at **www.codesys.com**

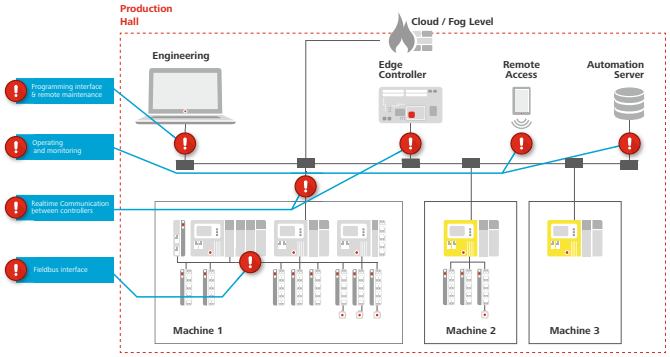

Figure 15: Main security attack vectors of an automation system

The CODESYS system offers the following security functions:

CODESYS Development System
- Encryption of the application source code with a password, dongle, or X.509 certificates.
- User management on the project level
- Encrypted communication between the CODESYS Development System and the PLC

CODESYS Runtime System
- User management for controller access
- Encryption and signing of the executable application code
- Operation modes for the executable application code
- Interactive login on the target device
- Easy exchange or recovery of controllers
- Encrypted OPC UA communication

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

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

CODESYS Automation Server
- Encapsulation of the devices in the local network: Data exchange with the Server exclusively via CODESYS Edge Gateway.
- Encrypted communication: Data exchange between the Server and CODESYS Edge Gateway 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 - the latter additionally secured via two-factor authentication.
- Total transparency of actions: Recording of accesses and changes via audit trail
- Know-how protection: Signing/encryption of source and compiled binary code via X.509 certificate, dongle, or password.
- Certified security: Regular security audits by external auditors

CODESYS Security Advisories

www.codesys.com/security

3.5.6 Weidmüller Software Tools

Weidmüller is also provider of the PROCON software family and ResMa. These software tools can be installed on third party Windows and Linux devices. To ensure a secure operation the following tips must been taken into account:

Best Security Practices for Weidmüller Software Tools

- **Secure the host-system:** The software tools PROCON-WEB SCADA and ResMa are designed to run on Windows-Devices. PROCON-WEB Embedded and PROCON-Connect are designed to run on Windows and Linux. The OS must be secured to ensure the integrity of all configurations and data that is stored on the device.
- **Use HTTPS instead of HTTP:** Different to ResMa, PROCON-WEB does not use HTTPS as default, it is recommended to activate HTTPS in the configuration to have an encrypted communication.
- **Change the default passwords:** Change the default admin and streaming passwords right after the installation.
- **Configure strong password policies:** To ensure save passwords, set the password policies according to our recommendation, see chapter “3.4.1 Strong Password”.
- **Setup User Management:** Use the User & Permission Management when creating an HMI Software. Secure your HMI with the built-in user management and use permissions in your project to protect different actions and view with different permissions.
- **Use Least Privilege Principle:** When creating the permission sets for different roles, ensure that only the necessary permissions are assigned.
- **Install Security updates:** When Weidmüller informs about vulnerabilities in the software, it is strongly recommended to install the provided security patch.

4. Appendix

4.1 Glossary

Term	Explanation
conduit	A conduit groups the elements that allow communication between two zones. Conduits provide security functions that enable secure communication and allow zones with different security levels to coexist. Typically, a conduit is realised by a router with a firewall.
CRA	**Cyber Resilience Act** EU security law for products with digital elements and communication functionality. CE relevant end of 2027.
CSIRT	**Computer Security Incident Response Team** The CSIRT is responsible for the vulnerability management on system level. See also PSIRT on product level
CSMS	**Cyber Security Management System** Term from IEC 62443. The term is synonymous with the term ISMS in the ISO 27001.
CSRS	Cyber Security Requirement Specification.
DMZ	**Demilitarised Zone** A DMZ network is an extra layer of security that enables enterprises to separate private networks from public Internet access and secure critical data.
DoS / DDoS	**(Distributed) Denial of Service attack** A DoS attack is a cyber-attack with which the attacker wants to prevent users from accessing network or computer resources.
ENISA	European Union Agency for Cybersecurity
IACS	**Industrial Automation and Control System** Term from the IEC 62443. IACSs consist of hardware, software and network components that are used to automate and monitor industrial production systems and their processes.
IDS	**Intrusion Detection System** An IDS uses certain patterns to detect attacks on computer systems or networks independently 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 series of standards is divided into different areas and describes both technical and procedural aspects of industrial cybersecurity. The series divides the industry into different roles: the operator, the integrators, and the manufacturers.
IEC 62443-3-3	This part of the IEC 62443 standard defines the system requirements for a secure system. It defines 5 security levels (4 with security functions; level 0 with no security).
IEC 62443-4-1	This part of the IEC 62443 standard defines what a secure development process for products 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.
ISA 62443	International Society of Automation (ISA) series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). ISA is similar to ANSI.
ISMS	**Information Security Management System** Term from ISO 27001. The term is synonymous with the term CSMS in the IEC62443.
IT	**Information Technology** Abbreviation for classic IT infrastructure such as MS Office, ERP, email, web server.
NIS / NIS2	**Network Information System Security** Term from EU law. NIS covers only critical infrastructure. NIS2 with extended scope for many other industry segments. NIS2 is in force with national laws October 2024
NIST	**National Institute of Standards and Technology** The institute is a non-regulatory agency within the U.S. Department of commerce that drives innovation by promoting the science of measurement, standards, and technology.
NIST CSF	**NIST Cybersecurity Framework** Today, the NIST CSF is still one of the most widely used security frameworks in the entire US industry.
OS	Abbrevation for Operating System e.g. Weidmüller u-OS
OT	**Operational Technology** Production infrastructure such as production machines and production IT infrastructure

Term	Explanation
PKI	**Public Key Infrastructure** A public key infrastructure is a hierarchical system for generating, distributing and verifying digital certificates.
PSIRT	**Product Security Incident Response Team** The PSIRT is responsible for the vulnerability management on product level. See also CSIRT on system level
RED / RED-DA	**Radio Equipment Directive (Delegated Act)** Term from EU law. In general, RED is valid for devices with radio functionality. The DA extension is valid for security functions. RED-DA with CE necessity from August 2025.
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 therefore 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 using real-time analysis and initiates appropriate countermeasures.
SL	**Security Level** The security level as defined in IEC 62443 describes the security requirements of a IT infrastructure. SL 0: No special requirements or protection needed. SL 1: Protection against unintentional or accidental misuse. SL 2: Protection against deliberate misuse using simple means with low resources, general skills, and low motivation. SL 3: Protection against deliberate misuse using sophisticated means with moderate resources, IACS-specific knowledge, and moderate motivation. See also IACS. SL 4: Protection against deliberate misuse using sophisticated means with extensive resources, IACS-specific knowledge, and high motivation. See also IACS.
SPDL	**Secure Product Development Lifecycle** Process description from the IEC 62443-4-1
VPN	**Virtual Private Network** The VPN refers to a virtual private (self-contained) communication network. Virtual in the sense that it is not a separate physical connection, but an existing communication network that is used as a transport medium. The VPN is used to connect subscribers of the existing communication network to another network.
zone	Network zones divide a system into homogeneous zones by grouping logical or physical systems with common security requirements. The security requirements are defined via security levels (SL).

Notes

Imprint: Weidmüller Interface GmbH & Co. KG, Klingenbergstraße 26, 32756 Detmold, Tel.: +49 5231 14280, E-Mail: weidmueller@weidmueller.de, www.weidmueller.de | Limited partnership (KG), Registered office: Detmold, Register court Lemgo HRA 2790 | General partner: Weidmüller Führungsgesellschaft mbH, Registered office: Detmold, Register court Lemgo HRB 3924, VAT ID no.: DE124599660 | Corporate Executive Management: 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, signal and data. We are at home in their industries and markets and know the technological challenges of tomorrow. We are therefore continuously developing innovative, sustainable and useful solutions for their individual needs. Together we set standards in Smart Industrial Connectivity.

Made in Germany

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
www.weidmueller.com

Personal support can
be found on our website:
www.weidmueller.com/contact

05/2025