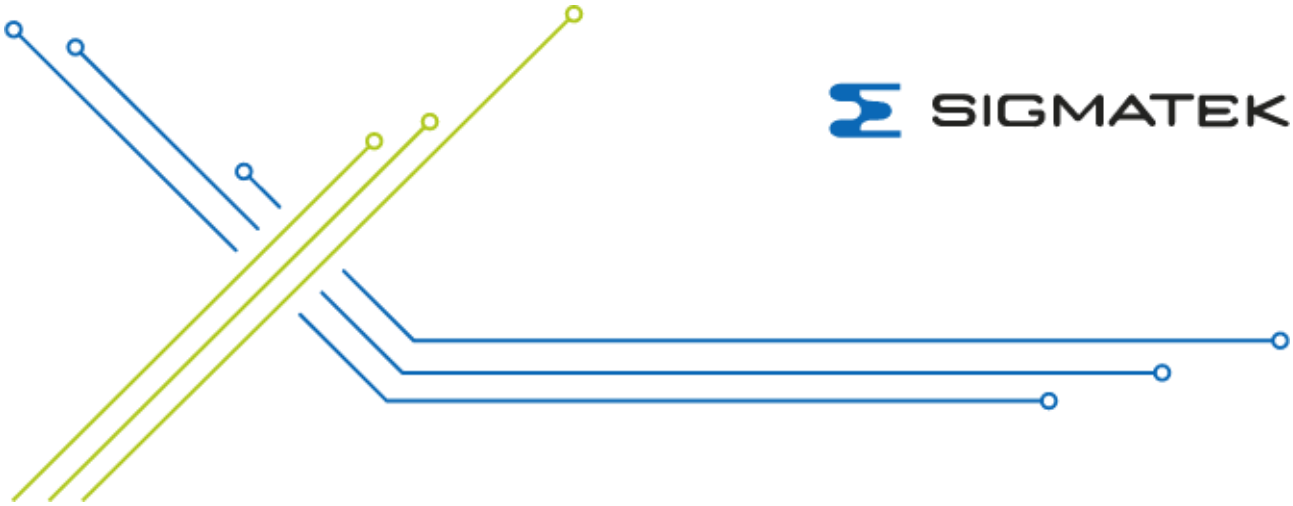
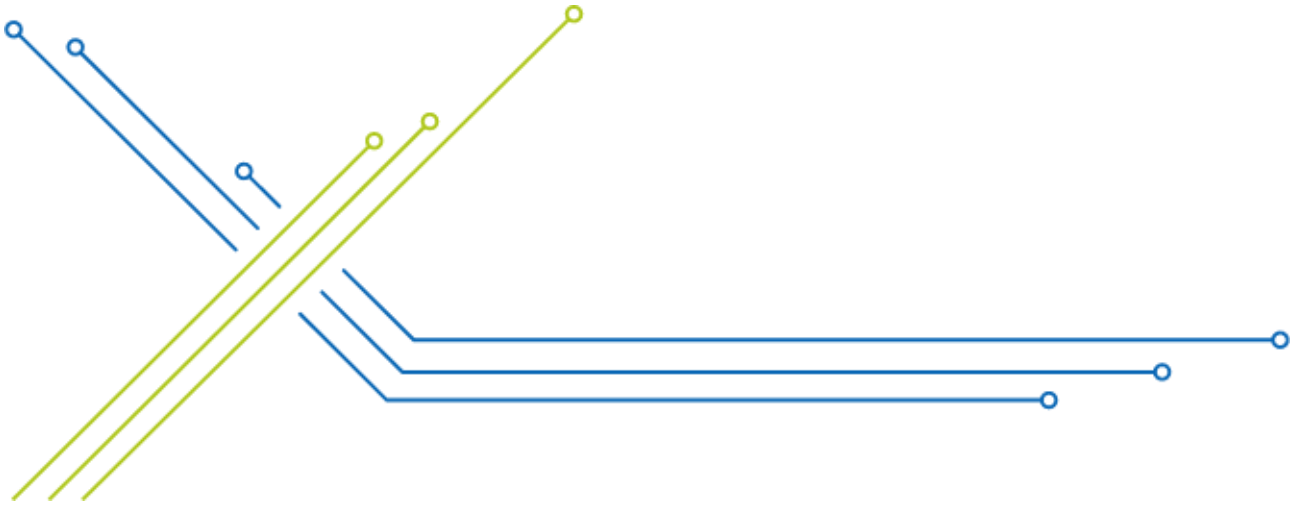


SIGMATEK

Cybersecurity

WHITE PAPER

Date of creation: 20.10.2025
Version date: 09.04.2026



Publisher:
SIGMATEK GmbH & Co KG
A-5112 Lamprechtshausen
Tel.: +43/6274/4321
Fax: +43/6274/4321-18

Email: office@sigmatek.at

www.sigmatek-automation.com

Contents

1 Introduction 2
2 Objectives of the Security Concept for SIGMATEK Automation Components 3
3 European Legal and Standards Framework for Cybersecurity 4
3.1 NIS2 Directive – Security of Network and Information Systems 4
3.2 Machinery Directive and Cyber Resilience Act 5
3.3 Standards as a benchmark for the state of the art in cybersecurity 5
3.4 Implications for manufacturers of automation components 6
4 Challenges & Specifics of Industrial OT Security 7
5 Threat Landscape & Attack Vectors 9
6 Risk analysis and assessment of cyber exposure 10
6.1 Security Assets in SIGMATEK Automation Systems 10
6.2 Cyber Exposure and Exposure Levels 11
6.3 Relationship between Exposure Level and Required Security Measures 14
7 Implementation Strategy of the Security Concept 15
7.1 Secure development processes for the systematic avoidance of vulnerabilities 15
7.2 Security by Design and Security by Default 16
7.3 Role of the operating system in the security architecture of automation components 17
7.4 Secure integration of SIGMATEK components into heterogeneous customer environments 20
7.5 Product Protection throughout the Entire Lifecycle 21
7.6 Prerequisites and Limitations of Update and Migration Capabilities 22
8 Summary 23

1 Introduction

The digitalization of industrial production is advancing rapidly. Modern automation systems are increasingly networked, integrate edge and cloud technologies, and communicate via open standard protocols. This development creates new opportunities for efficiency, flexibility, and innovation—but also poses significant new risks in the area of cybersecurity.

Industrial automation components, such as those developed and supplied by SIGMATEK, are now at the heart of complex production and control networks. At the same time, they are a prime target for cyberattacks: uncontrolled malware, industrial espionage, or targeted manipulation can compromise the availability, integrity, and confidentiality of industrial systems. Attacks on industrial automation can have far-reaching consequences—ranging from production downtime and economic losses to threats to workplace safety.

Against this backdrop, a comprehensive cybersecurity concept for automation components is not merely a technical requirement but a business-critical factor.

SIGMATEK is rising to this challenge and views cybersecurity as an integral part of the entire product lifecycle—from initial specification through manufacturing to long-term support.

This white paper describes the fundamental requirements, strategies, and measures SIGMATEK uses to address increasing security demands. It outlines practical approaches to integrating cybersecurity into industrial systems and provides an overview of technologies and concepts that help customers make their production environments future-proof and resilient.

SIGMATEK’s goal is to sustainably strengthen customer confidence in the digital transformation of industry through highly available, secure automation solutions.

2 Objectives of the Security Concept for SIGMATEK Automation Components

The security concept aims to design, integrate, and operate the automation components developed and supplied by SIGMATEK in such a way that they provide sustainable protection against cyber threats in industrial environments.

The focus is on effectively safeguarding the key protection goals of availability and integrity, as well as preventing cyberattacks from compromising functional safety.

The security concept follows a risk-based approach. The prioritization and design of security measures are based on a systematic risk analysis and assessment of the cyber exposure of the security assets in use. This methodological foundation is described in Chapter5 and ensures that measures are implemented in a manner that is appropriate, traceable, and proportional to the actual level of connectivity, accessibility, and attack surface.

In particular, the goal is to achieve:

1. Secure development processes that systematically avoid vulnerabilities and meet security standards.
2. To embed Security by Design and Security by Default in all products—without compromising the real-time capability, determinism, and functional safety of the systems.
3. To enable the secure integration of SIGMATEK components into heterogeneous customer environments through:
    - Protection mechanisms at the communication, access, and operating system levels
    - A clear separation of responsibilities between component manufacturers, machine manufacturers, and operators
4. Ensuring product protection throughout the entire lifecycle and support period, including:
    - Secure firmware updates and patching mechanisms
    - Protection concepts for legacy and existing systems
5. Promoting security awareness throughout the entire supply chain

In this way, the security concept creates a robust framework for systematically reducing cyber risks in industrial applications while simultaneously meeting the requirements for availability, performance, and functional safety in OT systems.

3 European Legal and Standards Framework for Cybersecurity

The development and operation of secure automation components are increasingly subject to binding regulatory requirements and technical standards. Cybersecurity is no longer exclusively a voluntary quality attribute but is explicitly addressed in both machinery legislation and horizontal product regulations.

This chapter presents the regulations and standards relevant to SIGMATEK automation components and outlines their scope of application and objectives. The focus is particularly on the Machinery Regulation (EU) 2023/1230 and the Cyber Resilience Act (Regulation (EU) 2024/2847). In addition, the NIS2 Directive (Directive (EU) 2022/2555) must also be taken into account as an overarching regulatory framework that establishes organizational and operational cybersecurity obligations for manufacturers and operators.

Given that certain aspects of the regulations and standards have not yet been definitively defined, official FAQ documents and standard interpretations by organizations such as the VDMA will be incorporated into the further development of this framework.
The aim of this chapter is to present the regulatory framework transparently and to establish a common basis for the subsequent risk, architecture, and implementation considerations.

3.1 NIS2 Directive – Security of Network and Information Systems

Directive (EU) 2022/2555 (NIS2) aims to ensure a high common level of cybersecurity within the European Union. The focus is on organizations of substantial or significant importance for critical and economically relevant services.
Unlike product-specific cybersecurity requirements, such as the Cyber Resilience Act, NIS2 is not directed at individual products but rather at companies and operational structures. It defines organizational, procedural, and technical requirements for the management of information and cybersecurity risks as well as for responding to security incidents.

This white paper primarily addresses the cybersecurity characteristics of automation products and their secure integration into machines and systems.
The NIS2 Directive is not directly applicable to individual products; however, it requires organizations to implement appropriate measures for the secure design of OT infrastructure, such as through risk-based segmentation of OT networks.

3.2 Machinery Directive and Cyber Resilience Act

In the future, cybersecurity requirements for automation components will stem from two complementary sets of European regulations:

- the **Machinery Regulation (EU) 2023/1230** and the
- **Cyber Resilience Act** (Regulation **(EU) 2024/2847**)

The Machinery Regulation specifically addresses cybersecurity in the context of functional safety. The focus here is on protecting safety-related functions from tampering and malfunctions that could endanger people. Accordingly, the cybersecurity requirements of the Machinery Regulation are limited to safety products and safety-related functions of machines.

In contrast, the Cyber Resilience Act takes a horizontal, cross-product approach. It defines binding cybersecurity requirements for all hardware and software products with digital elements, regardless of whether they perform a safety-related function.

3.3 Standards as a benchmark for the state of the art in cybersecurity

In addition to the mandatory legal requirements, there is a range of established European and international standards that reflect the recognized state of the art in cybersecurity.

These standards serve as a guide and reference framework for the implementation of technical and organizational security measures and support the interpretation of regulatory requirements.

Depending on the product type, function, and application context, the following standards are particularly relevant:

EN IEC 62443 – IT security for industrial automation systems

- The – as yet incomplete – EN IEC 62443 series of standards represents the central reference framework for cybersecurity in the industrial automation environment.
- It is generally applicable to all industrial control and automation components and covers requirements at the product, system, and process levels.
- The requirements for secure development formulated in the standard are used as the basis for designing the development process.

EN 50742 – Safety of machinery – Protection against tampering

- The pEN 50742 standard addresses protection against tampering with safety-related functions and applies exclusively to safety products in a machinery context.
- It forms an important interface between functional safety and cybersecurity by ensuring that safety-related functions are also protected against intentional or unintentional interference.

EN 18031-1 – Common safety requirements for radio equipment

- The EN 18031-1 standard defines fundamental cybersecurity requirements for radio equipment and, as a harmonized standard, is primarily situated within the context of the RED Directive.
- In terms of content, however, the standard does not explicitly limit itself to pure radio products, but rather describes generic security requirements for digital systems with communication interfaces.
- The standard thus complements the cybersecurity framework, particularly where automation components are used in networked system architectures.

The standards mentioned have different scopes and objectives, but together they form a consistent benchmark for the state of the art in cybersecurity. They are applied in the safety concept in a risk-oriented, product-specific, and context-dependent manner and supplement the mandatory requirements of the Machinery Regulation and the Cyber Resilience Act.

3.4 Implications for manufacturers of automation components

This has several significant implications for manufacturers of automation components:

- Cybersecurity must be considered and implemented both **in an exposure-based manner** within the security and application context (e.g., in conjunction with safety functions)

- as well as **across the entire lifecycle and across products** in accordance with the CRA.

- Technical safety measures must always be evaluated in the context of regulatory requirements and the recognized state of the art.

The following chapters build upon this legal and normative framework and derive concrete requirements for risk analysis, security architecture, and implementation strategy for SIGMATEK automation components.

4 Challenges & Specifics of Industrial OT Security

In contrast to traditional IT, cybersecurity in the field of industrial automation technology (Operational Technology, OT) faces its own unique conditions. For SIGMATEK, as a control system supplier that develops both hardware and software platforms for machine manufacturers, this presents specific challenges:

Long-term product lifecycles

Industrial control systems can remain in use for up to 20 years—significantly longer than typical IT components. Threats evolve dynamically. Security is not a static state but must be continuously monitored and adapted.

Heterogeneous customer environments

SIGMATEK customers operate control systems in a wide variety of infrastructure environments—from small businesses to highly automated corporations.

- Different network topologies
- Varying levels of maturity in IT/OT security
- Varying levels of knowledge and resources on the customer side

Functional safety vs. cybersecurity

Many SIGMATEK products are also used in safety-critical applications (e.g., emergency stop, drive enable).

- Safety functions must not be compromised by cybersecurity measures.
- Updates to certified safety components are subject to a strict approval process that also involves notified bodies (e.g., TÜV).
- Cybersecurity measures must be compliant with functional safety (e.g., deterministic behavior).

Real-Time Requirements & Performance

Some industrial processes require strict real-time requirements. Communication protocols (e.g., OPC UA, ...) must be security-enabled or protected by alternative measures while also being real-time capable.

- Encryption, firewalls, or certificate verification can increase latency or affect cycle times.
- Not all traditional IT security methods are technically feasible or practical (e.g., full disk encryption on controllers with real-time operating systems).

Shared Responsibility in the Supply Chain

- SIGMATEK supplies industrial controllers that are integrated into systems by machine manufacturers—ultimate responsibility lies with the machine manufacturer and the end user.

- SIGMATEK delivers controllers and software tools ex works with configurable security options, but cannot control the entire integration context.
- Roles and responsibilities (e.g., for patching, user management, network segmentation) must be clearly defined.

Legal & Regulatory Developments

Overarching regulatory requirements must be taken into account:

- Machinery Regulation (EU) 2023/1230
- EU Cyber Resilience Act (CRA)
- NIS2 Directive and associated national laws.

5 Threat Landscape & Attack Vectors

Industrial control systems (ICS) are increasingly becoming the focus of cyberattacks. While traditional IT systems have long been targets of attacks, production facilities, machines, and infrastructure components are also coming under fire as digitalization and networking advance. Attacks on Operational Technology (OT) can result not only in data loss but also in production downtime, property damage, or even risks to human safety.

Current Threat Landscape

The threat landscape for industrial systems has significantly worsened in recent years. Attackers are increasingly using targeted and technically sophisticated methods to exploit vulnerabilities in ICS environments. Key threats include:

- **Malware in production:** Trojans that specifically encrypt production systems and demand ransom (e.g., Lockbit, Ryuk)
- **Supply chain attacks:** Injection of malicious code via third-party systems or software vendors (e.g., SolarWinds)
- **Advanced Persistent Threats (APT):** Long-term, covert attacks by state-sponsored actors for industrial espionage or sabotage
- **Insider threats:** Misconduct or targeted manipulation by employees with access to critical systems

Typical attack vectors in ICS environments

Due to technical characteristics and organizational weaknesses, ICS environments offer numerous potential attack vectors:

Attack vector	Description
Uncontrolled remote access	Vulnerabilities in access protocols (compromised protocols)
Outdated systems & software	Operating systems that are no longer patched
USB and removable storage devices	Introduction of malware via operators or maintenance personnel
Open interfaces & protocols	Plaintext protocols, lack of authentication
Network sniffing & IP spoofing	Attacks on unfiltered or poorly segmented networks using spoofed IP addresses
Man-in-the-Middle (MitM)	Manipulation of communication between control components

6 Risk analysis and assessment of cyber exposure

Cybersecurity in automation technology is not an end in itself, but serves to protect the availability, integrity, and functional safety of machines and systems. A prerequisite for targeted protection is a thorough risk analysis that takes into account both the components used and their actual operating environment.

Modern machines consist of a multitude of heterogeneous security assets—from control CPUs and drive systems to HMIs, communication interfaces, and software services. However, their security risk is not static but depends largely on how heavily these components are networked and accessible from the outside.

To systematically assess this interconnectedness, an asset's cyber exposure is classified into exposure levels. These indicate the environment in which a component is located and the potential threats to which it is exposed. The following sections describe these exposure levels and demonstrate how appropriate security measures can be derived from them.

6.1 Security Assets in SIGMATEK Automation Systems

As part of the risk analysis, the first step is to identify those components whose compromise could affect the safety of a machine or system. These components are referred to as security assets.

Security assets are all elements worthy of protection that contribute to the control, monitoring, operation, or communication of a machine and whose manipulation could compromise availability, integrity, confidentiality, or functional safety. This includes both hardware and software components.

A key characteristic of security assets is that their cyber risk does not primarily arise from the component itself, but rather from its integration into the machine and network architecture.
The same PLC or HMI can—depending on the application scenario—pose a low or significant cyber risk.
For this reason, identifying security assets is merely the first step in risk analysis. The actual assessment is performed by examining their cyber exposure, which is systematically described in the next section using defined exposure levels.

6.2 Cyber Exposure and Exposure Levels

After identifying the relevant security assets, the second step of the risk analysis involves assessing their cyber exposure. Exposure describes how and through which access paths an asset is potentially accessible from the outside—and thus how likely cyberattacks are in the respective operational context.

EN 50742 uses the concept of “Exposure Levels EL0–EL4” for this purpose. This classification makes it possible to secure security assets not in a blanket “maximum” manner, but in a risk-oriented way. The higher the exposure level, the higher the requirements for protective measures, particularly with regard to access control, segmentation, monitoring, and cryptographic protection.

6.2.1 Definition of Exposure Levels

EL0 – Internal (completely within a physically enclosed system).
EL0 includes components that are located entirely within a closed enclosure/machine or control cabinet and are not accessible from the outside (except with a key or tool).

EL1 – Physical Access
EL1 describes interfaces and functions that are accessible via direct physical access to the machine, e.g., local service ports, HMI user interfaces, or connected engineering PCs.

EL2 – Segmented Machine Network
EL2 applies when assets are integrated into a local industrial OT network that connects multiple machines or related components and is typically operated in a segmented manner. Access is via defined network paths within a controlled area.

EL3 – Production Network (OT Network)
EL3 describes integration into a higher-level production or site network (OT), e.g., control rooms. This significantly increases the attack surface, as multiple systems, user groups, and operational processes are interconnected. Starting at EL3, simple network segmentation is no longer sufficient. Communication always runs through an intermediary instance that acts as a security gateway. Typical controlled gateways include, for example, firewalls, VPN gateways, and VPN routers.

EL4 – Public/Untrusted Network
EL4 encompasses any connection outside the operator’s direct control, particularly public networks and Internet-based services (e.g., cloud services, remote services via public networks).

A key point in exposure analysis is that a machine does not automatically correspond to a single exposure level. Within the same facility, individual assets may have different levels of exposure:
The assessment is therefore performed per security asset and per communication relationship, not exclusively at the machine level.

The exposure levels are used to derive appropriate security measures in order to:

- Justify security requirements in a transparent manner
- Allocate protective measures in a risk-oriented manner
- Systematically avoid over- or under-protection

The following diagram schematically depicts a machine with typical automation components and classifies them into exposure levels EL0 through EL3 based on their cyber exposure.

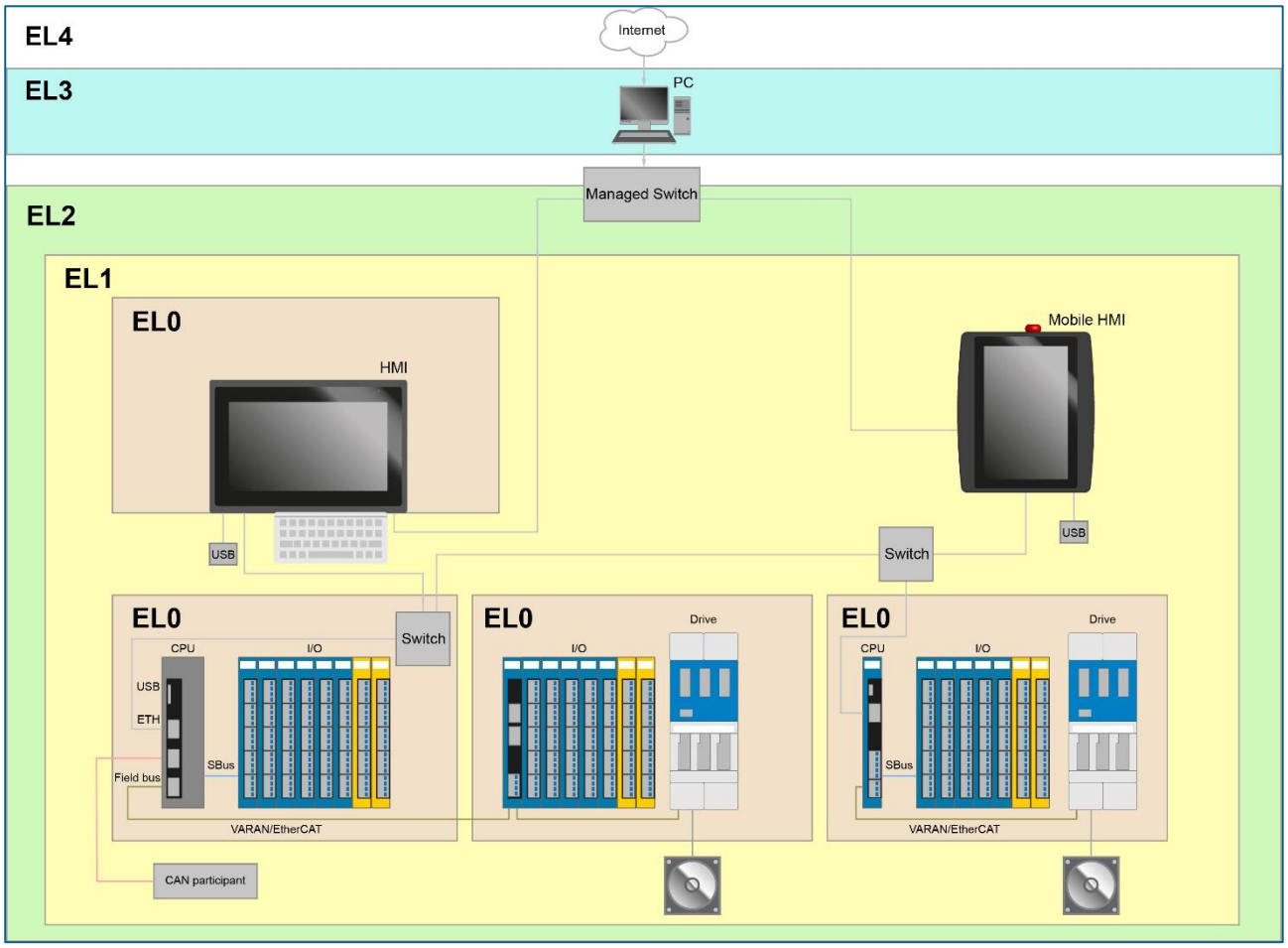
At the innermost core (EL0) are classic PLCs and control components installed within a closed control cabinet. These components are primarily protected against cyberattacks by physical safeguards. A key feature of EL0 is that all communication interfaces operate exclusively within the control cabinet.

As soon as communication extends beyond the control cabinet—for example, via a fieldbus such as CAN—physical protection remains in place, but an external communication link is established. The affected components are thus functionally assigned to Exposure Level 1.

EL1 includes devices whose cyber-exposed interfaces are accessible from the outside. Typical examples include HMIs, panel-mounted terminals, or cantilever terminals. Even if the electronics of a panel-mounted terminal and its interfaces are installed inside the machine or control cabinet, control elements such as virtual displays or accessible USB interfaces represent a communication interface to the outside world. These interfaces are thus subject to increased cyber exposure and must be classified as EL1.

EL2 represents a segmented OT network within the production facility. It forms the controlled and technically secured communication layer through which a secure connection to the higher-level OT network (EL3) is established. This communication relationship is typically implemented using so-called “managed switches,” which, in addition to pure data transmission, also provide integrated cybersecurity mechanisms such as network segmentation, access control, and monitoring, thereby enabling a controlled and secure connection between the networks.

Exposure Level 3 describes the factory’s OT network. Any communication connection from this area to public networks (the Internet) must additionally be secured via appropriate firewalls and security mechanisms to prevent unauthorized access.



EL0 => Control cabinet, components installed in the machine/system
EL1 => Machine/plant
EL2 => Segmented OT network
EL3 => Factory IT network
EL4 => Public network (Internet)

The diagram illustrates that security assets can be assigned different exposure levels depending on their integration and communication relationships. Each interface of an asset must be analyzed separately with regard to its cyber exposure, as security risks do not arise from the product itself, but from the respective communication relationship and its integration into the system architecture.

This becomes particularly clear in the example of the built-in terminal. While the internal electronics, including their communication interfaces, are assigned to exposure level EL0, the display with a virtual keyboard forms a user-side interface that is to be considered an EL1 interface.

Effective cybersecurity measures therefore do not arise solely at the fieldbus or protocol level, but primarily through architectural measures, targeted network segmentation, and clearly defined and controlled transitions between security zones.

6.3 Relationship between Exposure Level and Required Security Measures

The classification of a security asset into an Exposure Level (EL0–EL3) serves as a bridge between risk analysis and implementation. Appropriate, transparent, and proportionate security measures are derived from the actual level of exposure. As the Exposure Level increases, the attack surface grows—consequently, the requirements for access control, communication security, system hardening, and monitoring also increase.

Basic principle: “Security requirements follow exposure”

Security measures should be selected so that they:

- address actual access paths (physical, local, OT-wide, public)
- Clearly define trust boundaries (where does trust begin/end?)
- Increase complexity only where it provides a security benefit

A special case in OT is communication via real-time fieldbuses (e.g., EtherCAT/VARAN/CAN). These are typically unencrypted, which is why their protection at low exposure levels is primarily achieved through architectural measures (segmentation/isolation). At higher exposure levels, security must be ensured through secure gateways and controlled communication boundaries—for example, via Remote Access Routers, RAR 2400, RAR 2405, RAR 2410, etc. (see SIGMATEK website).

Not only components, but communication paths in particular are evaluated. Every connection across a trust boundary increases the need for protection. It follows that:

- Fieldbus segments remain (up to EL2) within a protected trust domain.
- Starting at EL3, transitions from the production network to the machine must be controlled (e.g., via VPN), logged (e.g., through logging), and cryptographically secured.
- In EL4, end-to-end identity, integrity, and authenticity are additionally mandatory for communication, software, and updates.

As cyber exposure increases, preventive security measures alone are no longer sufficient. Additional measures for detection and response are required.
This includes, in particular, systematic vulnerability management, which enables continuous assessment, treatment, and tracking of security vulnerabilities throughout the lifecycle.
This security capability is implemented and supported at SIGMATEK within the context of the current Salamander operating system platform with integrated security architecture. Earlier operating systems without system-level integrated security functions, on the other hand, do not support vulnerability management at the operating system level. Their use is therefore limited to applications with low cyber exposure or requires additional architectural protection measures outside the operating system.
The distinction between which operating system versions support an integrated security architecture and which are classified as legacy operating systems is explained in more detail in Chapter 7.3 .

7 Implementation Strategy of the Security Concept

This chapter describes how the derived security objectives are implemented in practice. The focus is on development processes, secure product design, secure integration into customer environments, product protection throughout the lifecycle, and security awareness along the supply chain. This creates a consistent framework that encompasses preventive, detective, and reactive measures.

7.1 Secure development processes for the systematic avoidance of vulnerabilities

SIGMATEK establishes secure development processes to systematically prevent vulnerabilities as early as the product development phase, guided by proven security standards, particularly IEC 62443-4-1.
The goal is to consistently incorporate security requirements—from requirements definition through design and implementation to verification, release, and maintenance.

This includes:

- **Threat modeling**: Potential security risks and vulnerabilities are systematically identified as early as the initial development phase through threat modeling and risk assessments.
- **Security checks**: Through regular code reviews and automated static code analysis, vulnerabilities are actively avoided in software development. The software is automatically checked for known vulnerabilities.
- **Development guidelines**: The implementation of best practices in software development, e.g., input validation, buffer overflow protection, and restricted privileges for programs and users.
- Defined **vulnerability process** (reporting, assessment, remediation, communication, traceability)

7.2 Security by Design and Security by Default

Security by Design means that security mechanisms are incorporated into the architecture and design of components from the outset, rather than being added as an afterthought. Security by Default ensures that products are shipped with a default configuration that supports an appropriate level of security and minimizes misconfigurations.

- **Security by Design**:
  - SIGMATEK follows the Security by Design approach, in which security functions are addressed early on in the design and architectural concept.
  - Communication relationships should be designed so that they operate in a secure mode by default.
- **Security by Default**:
  - Preconfigured, secure default settings (e.g., restrictive default permissions, minimization of open services) “Least privilege” principle: Permissions are initially limited and must be actively expanded.
  - All SIGMATEK products are shipped with configurable security options, such as password-protected admin access based on secure access mechanisms.

Security features are not only present but effective because they are built into the design and are sensibly preset as delivered.

7.3 Role of the operating system in the security architecture of automation components

The operating system forms the security foundation of every automation component. It controls startup and update processes, manages user and authorization models, provides communication services, and thus significantly determines the attack surface a device presents.

In practice, the cyber exposure of a CPU or an HMI is therefore not determined solely by the network connection, but to a large extent by the operating system's ability to control access, secure communication, and prevent tampering with software and configuration.

As exposure levels rise, the focus of security shifts. In low-exposure environments, security can be achieved in part through physical safeguards and network segmentation ("secure by environment"). At higher exposure levels, this approach is no longer sufficient, as external or site-wide communication relationships can only be managed if the end device itself has integrated security mechanisms.

These include, in particular, Secure Boot to ensure integrity during system startup, authenticated and integrity-protected updates, as well as hardened, cryptographically secured communication interfaces.

At SIGMATEK, the available security features vary depending on the version of the S operating system used.

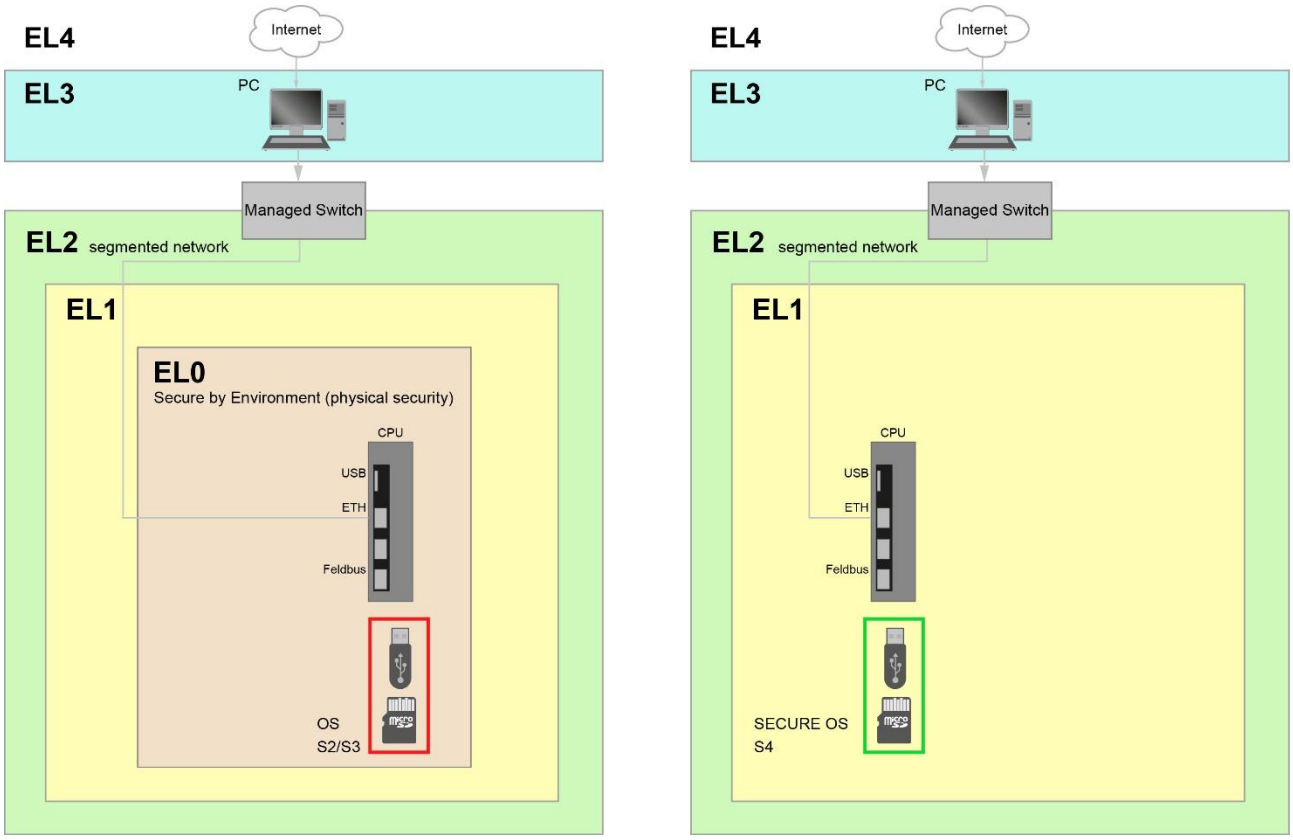
The following release versions are distinguished:

- S2 operating systems versions 09.01.xxx and 09.02.xxx
- S3 operating systems, versions 09.03.xxx and 09.04.xxx
- S4 operating systems starting with version 09.07.xxx

S2 and S3 were primarily developed for functional requirements in closed automation environments and have a limited integrated security architecture. These versions are also referred to as legacy operating systems.
S4 operating systems starting with release 09.07.xxx, on the other hand, are being specifically further developed and enhanced with system-level security functions. These form the basis for integrated security of the automation components and are referred to as S4 in the following.

This chapter explains how different operating system configurations determine the permissible scope of application for SIGMATEK automation components. Based on this, it demonstrates how cyber exposure can be controlled not only through environmental and network concepts, but increasingly through system-level security functions.

The following figure compares two different security approaches for SIGMATEK control systems and shows how the capabilities of the operating system used directly affect the permissible exposure levels (EL) and thus the integration and application possibilities within the overall system.



On the left is a SIGMATEK CPU running the S2 or S3 operating system. As described in previous chapters, these operating systems have limited cybersecurity functions.
The necessary protection for these systems is therefore primarily ensured by the environment (“secure by environment”):

- **Physical protective measures** (enclosed control cabinet, access only with a key or tool)
- **Limitation to low exposure levels** (EL0 / EL1)
- **Communication connections up to EL2**, provided that consistent network segmentation is implemented and the required cybersecurity protection can thereby be ensured at the system level.
- **Use of external security components** to architecturally secure higher exposure levels

Up to and including EL2, devices can be operated via Ethernet even without cryptographically secured communication, provided they are used exclusively in isolated, trusted network segments.

However, as soon as communication links beyond EL2 are required, the necessary protection can no longer be achieved through network segmentation alone. In these cases, the use of an additional external security component, e.g., RAR 2410, is required. This ensures cryptographic protection, authentication, and controlled transitions between different network zones.
Thus, S2 and S3 are generally limited to deployment scenarios with low to moderate cyber exposure, where there are no external communication links or only strictly controlled ones.

On the right side, the diagram shows a CPU with an S4 operating system that embeds security functions directly into the system design. As a result, security can no longer be achieved exclusively through the environment, but through integrated technical measures.

The secure operating system specifically extends the permissible scope of application for SIGMATEK products to higher exposure levels (EL3 and EL4), depending on the interfaces or services used, and thus supports modern OT and IT-related architectures.

The core security functions of the secure operating system are divided into three main areas:

Secure Online Interface
(Network and Communication Hardening)

The Secure Online Interface combines measures to secure network communication and online access, in particular:

- Default activation of modern encryption and authentication mechanisms for, e.g., LASAL connections
- Preconfigured firewall restrictions, e.g., whitelist-based communication approvals
- Optional pre-installation of an integrated VPN solution

These features enable (depending on the respective service) controlled and secure communication connections across trust boundaries and reduce the attack surface in external or site-wide networking.

Secure Update
(Authenticity of Software Updates)

The Secure Update mechanism ensures that only authorized software updates can be installed on the controller. This is supported by appropriate cryptographic methods, in particular digital signatures and their verified trust anchors.

Secure Boot
(Integrity)

Secure Boot is a security measure that ensures that only unmodified, authorized software is loaded during system startup. Among other things, the following are protected:

- Bootloader
- Kernel
- File system
- User partition

Together, Secure Online Interface, Secure Update, and Secure Boot form a consistent security foundation that systematically addresses key security objectives such as confidentiality, integrity, and authenticity, thereby creating the prerequisites for the secure operation of automation components in environments with increased exposure levels.

7.4 Secure integration of SIGMATEK components into heterogeneous customer environments

- **Protection mechanisms at the communication, access, and operating system levels**:

  SIGMATEK components were developed for integration into a network protected against unauthorized access and for installation in an access-protected area. The network or environment may be subject to threats such as unauthorized access, data manipulation, physical access, and tampering.

  It is the responsibility of the machine manufacturer or operator to conduct a risk analysis of the connections between SIGMATEK components and their integration into the overall infrastructure.

  This may result in measures such as: a restricted-access area, deactivation of Ethernet services and automatic address assignment, firewalls, VPNs, and IDS/IPS systems (Intrusion Detection/Prevention Systems) to ensure secure communication within a security-critical network.

- **Separation of Responsibilities**:
  - SIGMATEK (**component manufacturer**) is responsible for providing secure automation components and interfaces in accordance with the principles *of security by design and security by default*. This includes, in particular, the implementation of system-level security mechanisms as well as the provision of necessary security updates and patches for the respective product platform.
  - The **machine manufacturer** plays a central role in ensuring the cybersecurity of the entire machine. The following tasks fall specifically within its area of responsibility:
    - The machine manufacturer defines the machine's cyber exposure and determines which interfaces, services, and communication relationships are necessary and permissible for the intended use.
    - Through the development of customer-specific application software, the machine manufacturer plays a decisive role in determining which system-provided security functions are used, configured, or effectively applied.
    - The machine manufacturer ensures that the integration of security updates and patches does not adversely affect the machine's functional, safety-related, and application-specific requirements.
    - The operator is also responsible for ensuring that security patches are provided to the operator in an appropriate format so that they can be implemented as part of safe operation.
  - The **operator** is responsible for the safe operation of the machine throughout its entire lifecycle, based on the operating conditions and exposure levels defined by the machine manufacturer.

- The operator ensures that the machine is operated exclusively within the exposure levels defined by the machine manufacturer.
- The operator is responsible for implementing organizational and technical operational measures.
- The operator ensures the proper handling of security updates and patches.

7.5 Product Protection throughout the Entire Lifecycle

Cybersecurity is a continuous process throughout the entire product lifecycle—from delivery to the end of service life. In addition to preventive measures, update and patch capabilities, as well as the handling of legacy systems, are particularly crucial.

- **Secure firmware updates and patching mechanisms**:

  SIGMATEK makes new operating system versions available to the machine manufacturer on a portal to be defined.

  The implementation and verification of updates are the responsibility of the machine manufacturer.

- **Protection concepts for legacy and existing systems**:

  Legacy products without cybersecurity measures must be isolated from critical networks to minimize the risk of threats spreading. A legacy control system could run in its own network segment, separate from other modern systems, to prevent it from serving as an entry point for attacks on other systems.

- **Physical security isolation:**

  For critical legacy systems that do not offer modern security mechanisms, the machine manufacturer must implement physical security measures. This includes restricting access to the devices themselves and ensuring that only authorized personnel have physical access to the devices.

7.6 Prerequisites and Limitations of Update and Migration Capabilities

The ability to update an existing operating system to one with integrated security features depends largely on the characteristics of the hardware platform in use.

In particular, integrated cybersecurity features such as Secure Boot, cryptographically secured communication, as well as the authentication and integrity of software updates require corresponding system resources and hardware-based security mechanisms.

An upgrade is therefore only possible on devices that already run S4. Using S4 ensures that the respective hardware platform has the necessary computing, memory, and security resources to reliably implement the enhanced security features.

In contrast, an upgrade to S4 is not possible on devices running S2 or S3. These operating systems are used on older hardware platforms (e.g., EDGE2 technology) that do not provide the technical prerequisites required for modern cybersecurity mechanisms.

In such cases, the required (cyber) protection cannot be achieved through a software upgrade.
Instead, compensating measures must be implemented at the system and architectural levels, as described in the previous chapters, through consistent network segmentation, physical access restrictions, and the use of external security components.

The ability to update to S4 is therefore not a general software feature, but a hardware-dependent system characteristic that must be taken into account when selecting the platform and determining the intended exposure level classification.

8 Summary

The increasing networking and digitalization of industrial production systems requires a holistic understanding of cybersecurity. SIGMATEK addresses this development with a comprehensive security concept aimed at protecting automation components against cyber threats from the very beginning.

The focus is on integrating security measures throughout the entire product lifecycle—from initial specification through development and manufacturing to long-term support.

At the heart of the concept is the consistent implementation of secure development processes based on established standards.
A central methodological foundation is the assessment of cyber exposure via Exposure Levels (EL0–EL4). This assessment is conducted not only at the machine level, but also per security asset and per communication relationship. Security risks arise from the integration into the system architecture and the interfaces and services actually used. Effective cybersecurity arises from the interplay of architectural measures (segmentation, controlled transitions), system-level protection functions (access control, hardening, cryptography), and detective and reactive measures (e.g., vulnerability management).

Potential vulnerabilities are identified as early as the design phase and addressed through appropriate measures. Security mechanisms are integrated into the products from the outset and enabled by default, without compromising the real-time capability or functional safety of the systems.

Another focus is on the secure integration of SIGMATEK components into a wide variety of customer environments. This requires both technical protective measures at the communication and operating system levels as well as a clear separation of responsibilities between component manufacturers, machine builders, and operators. Even after commissioning, product protection is ensured through secure update mechanisms and concepts for handling legacy and existing systems.

Furthermore, SIGMATEK actively promotes security awareness throughout the entire supply chain.

With this holistic approach, SIGMATEK makes a decisive contribution to securing modern production systems and strengthens its customers’ confidence in the digital transformation of industry.

SIGMATEK will continuously adapt the further development of the security concept to new threat scenarios and technological trends.

The goal remains constant: to make automation "Made by SIGMATEK" permanently secure and future-proof.

Changes Chart

Change date	Affected page(s)	Chapter	Note	Version
20.10.2025		All		1.0
09.04.2026		3, 6, 7	Chapter 3: European Legal and Regulatory Framework for Cybersecurity Chapter 6: Risk Analysis and Assessment of Cyber Exposure Chapter 7: 7.3 Role of the Operating System in the Security Architecture of Automation Components 7.6 Prerequisites and Limitations of Update and Migration Capabilities	2.0