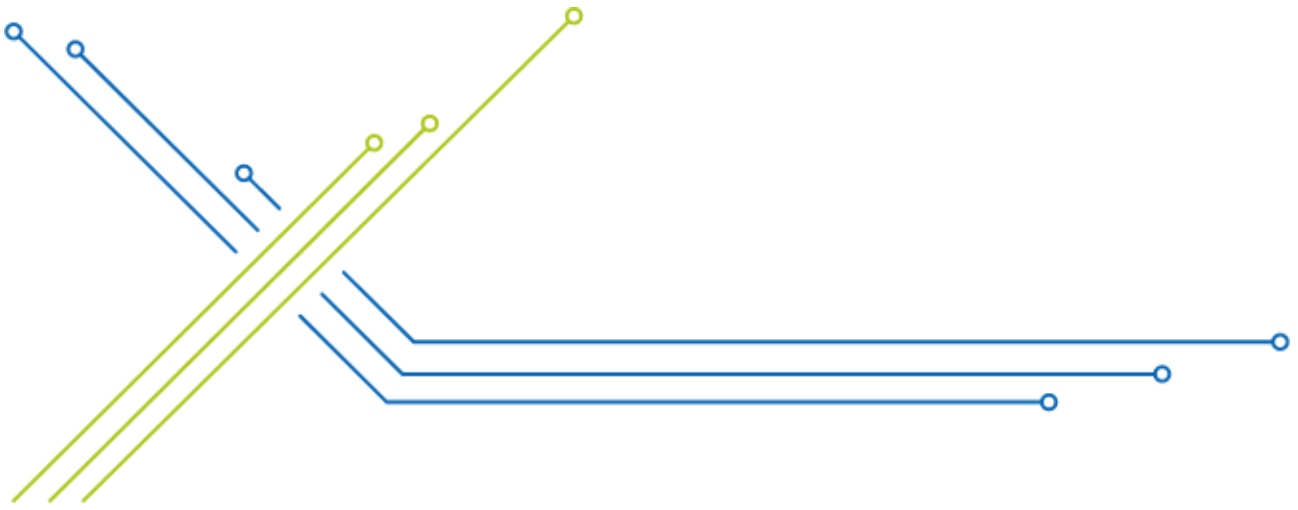


Cybersecurity

WHITEPAPER

Erstellungsdatum: 20.10.2025

Versionsdatum: 09.04.2026



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

Email: office@sigmatek.at

www.sigmatek-automation.com

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder in einem anderen Verfahren) ohne ausdrückliche Genehmigung reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Inhaltliche Änderungen behalten wir uns ohne Ankündigung vor. Die SIGMATEK GmbH & Co KG haftet nicht für technische oder drucktechnische Fehler in diesem Handbuch und übernimmt keine Haftung für Schäden, die auf die Nutzung dieses Handbuches zurückzuführen sind.

Copyright © 2026
SIGMATEK GmbH & Co KG

Inhalt

1	Einleitung	2
2	Zielsetzung des Sicherheitskonzepts für SIGMATEK Automatisierungskomponenten	3
3	Europäischer Rechts- und Normenrahmen für Cybersecurity	4
3.1	NIS2-Richtlinie – Sicherung von Netz- und Informationssystemen	4
3.2	Maschinenverordnung und Cyber Resilience Act.....	5
3.3	Normen als Maßstab für den Stand der Technik in der Cybersecurity	5
3.4	Konsequenzen für Hersteller von Automatisierungskomponenten.....	6
4	Herausforderungen & Besonderheiten der industriellen OT-Security	7
5	Bedrohungslage & Angriffsvektoren	9
6	Risikoanalyse und Bewertung der Cyber-Exponiertheit	10
6.1	Security Assets in SIGMATEK Automatisierungssystemen	10
6.2	Cyber-Exponiertheit und Exposure Levels	11
6.3	Zusammenhang zwischen Exposure Level und erforderlichen Security- Maßnahmen	14
7	Umsetzungs-Strategie des Sicherheitskonzeptes	15
7.1	Sichere Entwicklungsprozesse zur systematischen Vermeidung von Schwachstellen	15
7.2	Security by Design und Security by Default	16
7.3	Rolle des Betriebssystems in der Sicherheitsarchitektur von Automatisierungskomponenten.....	17
7.4	Sichere Integration der SIGMATEK-Komponenten in heterogene Kundenumgebungen.....	21
7.5	Produktschutz über den gesamten Lebenszyklus	22
7.6	Voraussetzungen und Grenzen der Update- und Migrationsfähigkeit	23
8	Zusammenfassung	24

1 Einleitung

Die Digitalisierung der industriellen Produktion schreitet rasant voran. Moderne Automatisierungssysteme werden zunehmend vernetzt, integrieren Edge- und Cloud-Technologien und kommunizieren über offene Standardprotokolle. Diese Entwicklung schafft neue Chancen für Effizienz, Flexibilität und Innovation – birgt jedoch auch erhebliche neue Risiken im Bereich der Cybersicherheit.

Industrielle Automatisierungskomponenten, wie sie von SIGMATEK entwickelt und geliefert werden, stehen heute im Zentrum komplexer Produktions- und Steuerungsnetzwerke. Gleichzeitig stehen Sie im Fokus in Bezug auf Cyberangriffen: unkontrollierte Schadsoftware, Industriespionage oder gezielte Manipulationen können die Verfügbarkeit, Integrität und Vertraulichkeit industrieller Systeme beeinflussen. Angriffe auf die industrielle Automatisierung können weitreichende Folgen haben – von Produktionsstillständen über wirtschaftliche Schäden bis hin zu Gefährdungen der Arbeitssicherheit.

Vor diesem Hintergrund wird ein umfassendes Cybersecurity-Konzept für Automatisierungskomponenten nicht nur zur technischen Anforderung, sondern zum geschäftskritischen Faktor.

SIGMATEK stellt sich dieser Herausforderung und versteht Cybersecurity als integraler Bestandteil des gesamten Produktlebenszyklus – von der ersten Spezifikation über die Fertigung bis zum langfristigen Support.

Dieses Whitepaper beschreibt die grundlegenden Anforderungen, Strategien und Maßnahmen, mit denen SIGMATEK den steigenden Sicherheitsanforderungen begegnet. Es zeigt praxisnahe Ansätze zur Integration von Cybersecurity in industrielle Systeme und bietet einen Überblick über Technologien und Konzepte, die Kunden dabei unterstützen, ihre Produktionsumgebungen zukunftssicher und resilient zu gestalten.

Ziel von SIGMATEK ist es, mit hochverfügbaren, sicheren Automatisierungslösungen das Vertrauen der Kunden in die digitale Transformation der Industrie nachhaltig zu stärken.

2 Zielsetzung des Sicherheitskonzepts für SIGMATEK Automatisierungskomponenten

Das Sicherheitskonzept verfolgt das Ziel, die von SIGMATEK entwickelten und gelieferten Automatisierungskomponenten so zu gestalten, zu integrieren und zu betreiben, dass sie einen nachhaltigen Schutz gegen Cyberbedrohungen im industriellen Umfeld bieten.

Im Mittelpunkt steht dabei die wirksame Absicherung der wesentlichen Schutzziele Verfügbarkeit, Integrität sowie die Vermeidung von Beeinträchtigungen der funktionalen Sicherheit durch Cyberangriffe.

Das Sicherheitskonzept folgt einem risikoorientierten Ansatz. Die Priorisierung und Ausgestaltung von Sicherheitsmaßnahmen erfolgt auf Basis einer systematischen Risikoanalyse und Bewertung der Cyber-Exponiertheit der eingesetzten Security Assets. Diese methodische Grundlage wird in Kapitel 5 beschrieben und stellt sicher, dass Maßnahmen angemessen, nachvollziehbar und proportional zur tatsächlichen Vernetzung, Zugänglichkeit und Angriffsfläche umgesetzt werden.

Dabei wird insbesondere das Ziel verfolgt:

1. Sichere Entwicklungsprozesse, die systematisch Schwachstellen vermeiden und Sicherheitsstandards erfüllen.
2. Security by Design und Security by Default in allen Produkten zu verankern – ohne die Echtzeitfähigkeit, Deterministik und funktionale Sicherheit der Systeme zu beeinträchtigen.
3. Sichere Integration der SIGMATEK-Komponenten in heterogene Kundenumgebungen zu ermöglichen, durch:
 - Schutzmechanismen auf Kommunikations-, Zugriffs- und Betriebssystemebene
 - Klare Trennung von Verantwortlichkeiten zwischen Komponenten-Hersteller, Maschinenhersteller und Betreiber
4. Produktschutz über den gesamten Lebenszyklus und Unterstützungszeitraum sicherzustellen, inklusive:
 - Sichere Firmware-Updates und Patching-Mechanismen
 - Schutzkonzepte für Alt- und Bestandssysteme
5. Sicherheitsbewusstsein entlang der gesamten Lieferkette zu fördern

Damit schafft das Sicherheitskonzept einen belastbaren Rahmen, um Cyber-Risiken in industriellen Anwendungen systematisch zu reduzieren und gleichzeitig die Anforderungen an Verfügbarkeit, Performance und funktionale Sicherheit in OT-Systemen zu erfüllen.

3 Europäischer Rechts- und Normenrahmen für Cybersecurity

Die Entwicklung und der Betrieb sicherer Automatisierungskomponenten stehen zunehmend im Einflussbereich verbindlicher regulatorischer Anforderungen und technischer Normen. Cybersecurity ist dabei nicht mehr ausschließlich eine freiwillige Qualitätseigenschaft, sondern wird sowohl im Maschinenrecht als auch in horizontalen Produktvorschriften explizit adressiert.

Dieses Kapitel stellt die für SIGMATEK Automatisierungskomponenten relevanten Verordnungen und Normen vor und ordnet deren Anwendungsbereich sowie Zielsetzung ein. Im Fokus stehen dabei insbesondere die Maschinenverordnung (EU) 2023/1230 sowie der Cyber Resilience Act (Verordnung (EU) 2024/2847). Ergänzend ist dabei auch die NIS2-Richtlinie (Richtlinie (EU) 2022/2555) als übergeordneter regulatorischer Rahmen zu berücksichtigen, der organisatorische und betriebliche Cybersecurity-Pflichten für Hersteller- und Betreiberorganisationen festlegt.

Vor dem Hintergrund, dass einzelne Aspekte der Verordnungen und Normen derzeit noch nicht abschließend definiert sind, werden offizielle FAQ-Dokumente und Normauslegungen durch z.B. VDMA in die weitere Ausgestaltung berücksichtigt. Ziel des Kapitels ist es, den regulatorischen Rahmen transparent darzustellen und eine gemeinsame Grundlage für die nachfolgenden Risiko-, Architektur- und Umsetzungsbetrachtungen zu schaffen.

3.1 NIS2-Richtlinie – Sicherung von Netz- und Informationssystemen

Die Richtlinie (EU) 2022/2555 (NIS2) verfolgt das Ziel, ein hohes gemeinsames Cybersicherheitsniveau innerhalb der Europäischen Union sicherzustellen. Im Fokus stehen dabei Organisationen mit wesentlicher oder wichtiger Bedeutung für kritische und wirtschaftlich relevante Dienstleistungen.

Im Gegensatz zu produktbezogenen Cybersecurity-Anforderungen, wie dem Cyber Resilience Act, richtet sich NIS2 nicht an einzelne Produkte, sondern an Unternehmen und Betreiberstrukturen. Sie definiert organisatorische, prozessuale und technische Anforderungen an das Management von Informations- und Cybersicherheitsrisiken sowie an die Reaktion auf Sicherheitsvorfälle.

Dieses Whitepaper adressiert primär die Cybersecurity-Eigenschaften von Automatisierungsprodukten sowie deren sichere Integration in Maschinen und Anlagen. Die NIS2-Richtlinie ist nicht unmittelbar auf einzelne Produkte anwendbar, verpflichtet jedoch Organisationen, angemessene Maßnahmen zur sicheren Ausgestaltung der OT-Infrastruktur umzusetzen, etwa durch eine risikobasierte Segmentierung von OT-Netzen.

3.2 Maschinenverordnung und Cyber Resilience Act

Die Cybersecurity-Anforderungen an Automatisierungskomponenten ergeben sich künftig aus zwei komplementären europäischen Regelwerken:

- der **Maschinenverordnung (EU) 2023/1230** und dem
- **Cyber Resilience Act** (Verordnung (EU) 2024/2847)

Die Maschinenverordnung adressiert Cybersecurity gezielt im Kontext der funktionalen Sicherheit. Der Fokus liegt dabei auf dem Schutz sicherheitsrelevanter Funktionen vor Manipulationen und Fehlverhalten, die zu einer Gefährdung von Personen führen könnten. Entsprechend beschränken sich die Cybersecurity-Anforderungen der Maschinenverordnung auf Safety-Produkte und sicherheitsbezogene Funktionen von Maschinen.

Der Cyber Resilience Act verfolgt demgegenüber einen horizontalen, produktübergreifenden Ansatz. Er definiert verbindliche Cybersecurity-Anforderungen für alle Hardware- und Softwareprodukte mit digitalen Elementen, unabhängig davon, ob diese eine sicherheitsgerichtete Funktion erfüllen.

3.3 Normen als Maßstab für den Stand der Technik in der Cybersecurity

Ergänzend zu den verbindlichen gesetzlichen Anforderungen existiert eine Reihe etablierter europäischer und internationaler Normen, die den anerkannten Stand der Technik im Bereich Cybersecurity widerspiegeln.

Diese Normen dienen als Orientierungs- und Referenzrahmen für die Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen und unterstützen die Auslegung regulatorischer Anforderungen.

Je nach Produktart, Funktion und Einsatzkontext sind insbesondere die folgenden Normen relevant:

EN IEC 62443 – IT-Sicherheit für industrielle Automatisierungssysteme

- Die – noch unvollständige - Normenreihe EN IEC 62443 stellt den zentralen Referenzrahmen für Cybersecurity im industriellen Automatisierungsumfeld dar.
- Sie ist grundsätzlich auf alle industriellen Steuerungs- und Automatisierungskomponenten anwendbar und deckt Anforderungen auf Produkt-, System- und Prozessebene ab.
- Die in der Norm formulierten Anforderungen an eine sichere Entwicklung werden als Grundlage für die Ausgestaltung des Entwicklungsprozesses herangezogen.

pEN 50742 – Safety of machinery – Protection against corruption

- Die Norm pEN 50742 adressiert den Schutz vor Manipulation sicherheitsrelevanter Funktionen und gilt ausschließlich für Safety-Produkte im Maschinenkontext.
- Sie bildet eine wichtige Schnittstelle zwischen funktionaler Sicherheit und Cybersecurity, indem sie sicherstellt, dass sicherheitsgerichtete Funktionen auch gegenüber absichtlicher oder unbeabsichtigter Beeinflussung geschützt sind.

EN 18031-1 – Gemeinsame Sicherheitsanforderungen für Funkanlagen

- Die Norm EN 18031-1 definiert grundlegende Cybersecurity-Anforderungen für Funkanlagen und ist als harmonisierte Norm primär im Kontext der RED-Richtlinie verortet.
- Inhaltlich adressiert die Norm jedoch keine explizite Abgrenzung auf reine Funkprodukte, sondern beschreibt generische Sicherheitsanforderungen für digitale Systeme mit Kommunikationsschnittstellen.
- Die Norm ergänzt somit den Cybersecurity-Rahmen insbesondere dort, wo Automatisierungskomponenten in vernetzten Systemarchitekturen eingesetzt werden.

Die genannten Normen haben unterschiedliche Anwendungsbereiche und Zielsetzungen, bilden in ihrer Gesamtheit jedoch einen konsistenten Maßstab für den Stand der Technik im Bereich Cybersecurity. Sie werden im Sicherheitskonzept risikoorientiert, produktspezifisch und kontextabhängig herangezogen und ergänzen die verbindlichen Anforderungen aus Maschinenverordnung und Cyber Resilience Act.

3.4 Konsequenzen für Hersteller von Automatisierungskomponenten

Für Hersteller von Automatisierungskomponenten ergeben sich daraus mehrere wesentliche Konsequenzen:

- Cybersecurity muss sowohl **exposure-basiert** im Sicherheits- und Anwendungskontext (z. B. im Zusammenspiel mit Safety-Funktionen)
- als auch **lebenszyklus- und produktübergreifend** im Sinne des CRA betrachtet und umgesetzt werden.
- Technische Sicherheitsmaßnahmen sind dabei stets im Zusammenhang mit regulatorischen Anforderungen und dem anerkannten Stand der Technik zu bewerten.

Die folgenden Kapitel bauen auf diesem rechtlichen und normativen Rahmen auf und leiten daraus konkrete Anforderungen an Risikoanalyse, Sicherheitsarchitektur und Umsetzungsstrategie für SIGMATEK Automatisierungskomponenten ab.

4 Herausforderungen & Besonderheiten der industriellen OT-Security

Im Gegensatz zur klassischen IT ist die Cybersicherheit im Bereich der industriellen Automatisierungstechnik (Operational Technology, OT) mit ganz eigenen Rahmenbedingungen konfrontiert. Für SIGMATEK als Steuerungslieferant, der sowohl Hardware als auch Softwareplattformen für Maschinenhersteller entwickelt, ergeben sich daraus spezifische Herausforderungen:

Langfristige Produktlebenszyklen

Industrielle Steuerungen können bis zu 20 Jahre im Einsatz sein – deutlich länger als typische IT-Komponenten. Bedrohungen entwickeln sich dynamisch. Sicherheit ist kein fester Zustand, sondern muss laufend überwacht und angepasst werden.

Heterogene Kundenumgebungen

SIGMATEK-Kunden betreiben Steuerungen in sehr unterschiedlichen Infrastrukturmgebungen – vom Kleinbetrieb bis zum hochautomatisierten Konzern.

- Unterschiedliche Netzwerktopologien
- Unterschiedlicher Reifegrad in der IT-/OT-Security
- Unterschiedliches Wissen & Ressourcen auf Kundenseite

Funktionale Sicherheit vs. Cybersicherheit

Viele SIGMATEK-Produkte kommen auch in sicherheitsgerichteten Anwendungen zum Einsatz (z. B. Not-Halt, Antriebsfreigabe).

- Sicherheitsfunktionen dürfen durch Cybermaßnahmen nicht beeinträchtigt werden.
- Das Update von zertifizierten Sicherheitskomponenten unterliegt einem strengen Freigabeprozess, der auch notifizierende Stellen (z.B. TÜV) mitberücksichtigt.
- Cybersecurity-Maßnahmen müssen konform zur funktionalen Sicherheit sein (z. B. deterministisches Verhalten).

Echtzeitanforderungen & Performance

Manche Industrieprozesse erfordern harte Echtzeitanforderungen. Kommunikationsprotokolle (z. B. OPC UA, ...) müssen security-fähig oder durch alternative Maßnahmen geschützt werden und gleichzeitig echtzeitfähig sein.

- Verschlüsselung, Firewalls oder Zertifikatsprüfung können Latenz erhöhen oder Taktzeiten beeinflussen.
- Nicht alle klassischen IT-Security-Methoden sind technisch realisierbar oder sinnvoll (z. B. Full Disk Encryption auf Steuerungen mit Echtzeitbetriebssystemen).

Verantwortungsteilung in der Lieferkette

- SIGMATEK liefert Industriesteuerungen, die von Maschinenherstellern in Anlagen integriert werden – die Endverantwortung liegt beim Maschinenhersteller und beim Endanwender.
- SIGMATEK liefert Steuerungen und Software-Tools ab Werk mit einstellbaren Sicherheitsoptionen, aber kann nicht den gesamten Integrationskontext kontrollieren.
- Rollen und Zuständigkeiten (z. B. für Patching, Benutzerverwaltung, Netzwerksegmentierung) müssen eindeutig definiert werden.

Rechtliche & normative Entwicklungen

Übergreifende regulatorische Anforderungen sind zu berücksichtigen:

- Maschinenverordnung (EU) 2023/1230
- EU Cyber Resilience Act (CRA)
- NIS2-Richtlinie und zugehörige nationale Gesetze.

5 Bedrohungslage & Angriffsvektoren

Industrielle Steuerungssysteme (ICS) stehen zunehmend im Fokus von Cyberangriffen. Während klassische IT-Systeme schon lange Ziel von Angriffen sind, rücken mit zunehmender Digitalisierung und Vernetzung auch Produktionsanlagen, Maschinen und Infrastrukturkomponenten ins Visier. Angriffe auf die Operational Technology (OT) können nicht nur Datenverluste, sondern auch Produktionsstillstände, Sachschäden oder gar Gefährdungen für Menschen zur Folge haben.

Aktuelle Bedrohungslage

Die Bedrohungslage für industrielle Systeme hat sich in den letzten Jahren signifikant verschärft. Angreifer nutzen immer häufiger gezielte und technisch ausgefeilte Methoden, um Schwachstellen in ICS-Umgebungen auszunutzen. Zu den zentralen Bedrohungen zählen:

- **Schadsoftware in der Produktion:** Trojaner, die gezielt Produktionssysteme verschlüsseln und Lösegeldforderungen stellen (z. B. Lockbit, Ryuk)
- **Supply-Chain-Angriffe:** Einschleusung von Schadcode über Drittsysteme oder Softwarelieferanten (z. B. SolarWinds)
- **Advanced Persistent Threats (APT):** Langfristige, verdeckte Angriffe durch staatlich unterstützte Akteure zur Industriespionage oder Sabotage
- **Insider-Bedrohungen:** Fehlverhalten oder gezielte Manipulation durch Mitarbeitende mit Zugriff auf kritische Systeme

Typische Angriffsvektoren in ICS-Umgebungen

Aufgrund technischer Eigenheiten und organisatorischer Schwächen bieten ICS-Umgebungen zahlreiche potenzielle Angriffsvektoren:

Angriffsvektor	Beschreibung
Unkontrollierter Fernzugriff	Schwachstellen in Zugriffsprotokollen (Kompromittierte Protokolle)
Veraltete Systeme & Software	Betriebssysteme, die nicht mehr gepatcht werden
USB- und Wechseldatenträger	Einbringung von Schadsoftware über Bediener oder Wartungspersonal
Offene Schnittstellen & Protokolle	Klartext-Protokolle, fehlende Authentifizierung
Netzwerk-Sniffing & IP Spoofing	Angriffe auf ungefilterte oder schlecht segmentierte Netzwerke mittels gefälschter IP-Adresse
Man-in-the-Middle (MitM)	Manipulation der Kommunikation zwischen Steuerungskomponenten

6 Risikoanalyse und Bewertung der Cyber-Exponiertheit

Cybersecurity in der Automatisierungstechnik ist kein Selbstzweck, sondern dient dem Schutz von Verfügbarkeit, Integrität und funktionaler Sicherheit von Maschinen und Anlagen. Voraussetzung für eine zielgerichtete Absicherung ist eine fundierte Risikoanalyse, die sowohl die eingesetzten Komponenten als auch deren reale Einsatzumgebung berücksichtigt.

Moderne Maschinen bestehen aus einer Vielzahl heterogener Security Assets – von Steuerungs-CPU's und Antriebssystemen über HMIs bis hin zu Kommunikationsschnittstellen und Software-Services. Deren Sicherheitsrisiko ist jedoch nicht statisch, sondern hängt wesentlich davon ab, wie stark diese Komponenten vernetzt und von außen erreichbar sind.

Zur systematischen Bewertung dieser Vernetzung wird die Cyber-Exponiertheit eines Assets in Form von Exposure Levels klassifiziert. Diese geben an, in welchem Umfeld sich eine Komponente befindet und welchen potenziellen Bedrohungen sie ausgesetzt ist. Die folgenden Abschnitte beschreiben diese Exposure Levels und zeigen, wie daraus angemessene Sicherheitsmaßnahmen abgeleitet werden können.

6.1 Security Assets in SIGMATEK Automatisierungssystemen

Im Rahmen der Risikoanalyse werden zunächst jene Komponenten identifiziert, deren Kompromittierung Auswirkungen auf die Sicherheit einer Maschine oder Anlage haben kann. Diese Komponenten werden als Security Assets bezeichnet.

Security Assets sind alle schützenswerte Elemente, die zur Steuerung, Überwachung, Bedienung oder Kommunikation einer Maschine beitragen und deren Manipulation die Verfügbarkeit, Integrität, Vertraulichkeit oder die funktionale Sicherheit beeinträchtigen kann. Dazu zählen Hardware- als auch Softwarekomponenten.

Ein wesentliches Merkmal von Security Assets ist, dass ihr Cyber-Risiko nicht primär durch die Komponente selbst entsteht, sondern durch deren Integration in die Maschinen- und Netzwerkarchitektur.

Derselbe PLC oder dasselbe HMI kann – je nach Einsatzszenario – ein niedriges oder ein erhebliches Cyber-Risiko darstellen.

Aus diesem Grund bildet die Identifikation der Security Assets lediglich den ersten Schritt der Risikoanalyse. Die tatsächliche Bewertung erfolgt durch die Betrachtung ihrer Cyber-Exponiertheit, welche im nächsten Abschnitt anhand definierter Exposure Levels systematisch beschrieben wird.

6.2 Cyber-Exponiertheit und Exposure Levels

Nach der Identifikation der relevanten Security Assets erfolgt im zweiten Schritt der Risikoanalyse die Bewertung ihrer Cyber-Exponiertheit. Die Exponiertheit beschreibt, wie und über welche Zugriffswege ein Asset potenziell von außen erreichbar ist – und damit, wie wahrscheinlich Cyberangriffe im jeweiligen Einsatzkontext sind.

Die EN 50742 verwendet hierfür das Konzept der „Exposure Levels EL0–EL4“. Diese Klassifizierung ermöglicht es, Security Assets nicht pauschal „maximal“ abzusichern, sondern risikoorientiert. Je höher das Exposure Level, desto höher sind die Anforderungen an Schutzmaßnahmen, insbesondere hinsichtlich Zugangskontrolle, Segmentierung, Monitoring sowie kryptografischer Absicherung.

6.2.1 Definition der Exposure Levels

EL0 – Intern (vollständig innerhalb eines physikalisch geschlossenen Systems). EL0 umfasst Komponenten, die sich vollständig innerhalb eines geschlossenen Gehäuses/Maschine bzw. Schaltschranks befinden und von außen nicht zugänglich sind (außer mit Schlüssel oder Werkzeug).

EL1 – Physischer Zugriff

EL1 beschreibt Schnittstellen und Funktionen, die durch direkten physischen Zugriff auf die Maschine erreichbar sind, z. B. lokale Service-Ports, HMI-Bedienoberflächen oder angeschlossene Engineering-PCs.

EL2 – Segmentiertes Maschinen-Netzwerk

EL2 liegt vor, wenn Assets in ein lokales industrielles OT-Netzwerk eingebunden sind, das mehrere Maschinen bzw. zusammengehörige Komponenten verbindet und typischerweise segmentiert betrieben wird. Der Zugriff erfolgt über definierte Netzwerkpfade innerhalb eines kontrollierten Bereichs.

EL3 – Produktionsnetz (OT-Netzwerk)

EL3 beschreibt die Einbindung in ein übergeordnetes Produktions- oder Standortnetzwerk (OT), z. B. Leitstände. Damit steigt die Angriffsfläche deutlich, da mehrere Systeme, Benutzergruppen und Betriebsprozesse gekoppelt sind. Ab EL3 reicht eine reine Netzwerksegmentierung nicht mehr aus. Die Kommunikation läuft immer über eine zwischengeschaltete Instanz, die als Sicherheits-Schleuse fungiert. Typische kontrollierte Übergänge sind z. B. Firewall, VPN-Gateway/VPN-Router.

EL4 – Öffentliches/nicht vertrauenswürdigenes Netzwerk

EL4 umfasst jede Anbindung außerhalb der unmittelbaren Kontrolle des Betreibers, insbesondere öffentliche Netze und Internetbasierte Services (z. B. Cloud-Dienste, Remote-Service über öffentliche Netze).

Ein zentraler Punkt der Exposure-Betrachtung ist, dass eine Maschine nicht automatisch nur einem einzigen Exposure Level entspricht. Innerhalb derselben Anlage können einzelne Assets unterschiedlich exponiert sein:

Die Bewertung erfolgt daher pro Security Asset und pro Kommunikationsbeziehung, nicht ausschließlich auf Maschinenebene.

Die Exposure Levels dienen der Ableitung angemessener Sicherheitsmaßnahmen, um:

- Sicherheitsanforderungen nachvollziehbar zu begründen
- Schutzmaßnahmen risikoorientiert zuzuordnen
- Über- bzw. Unter-Absicherung systematisch zu vermeiden

Die folgende Grafik stellt schematisch eine Maschine mit typischen Automatisierungskomponenten dar und ordnet diese entsprechend ihrer Cyber-Exponiertheit (Cyber Exposure) den Exposure Levels EL0 bis EL3 zu.

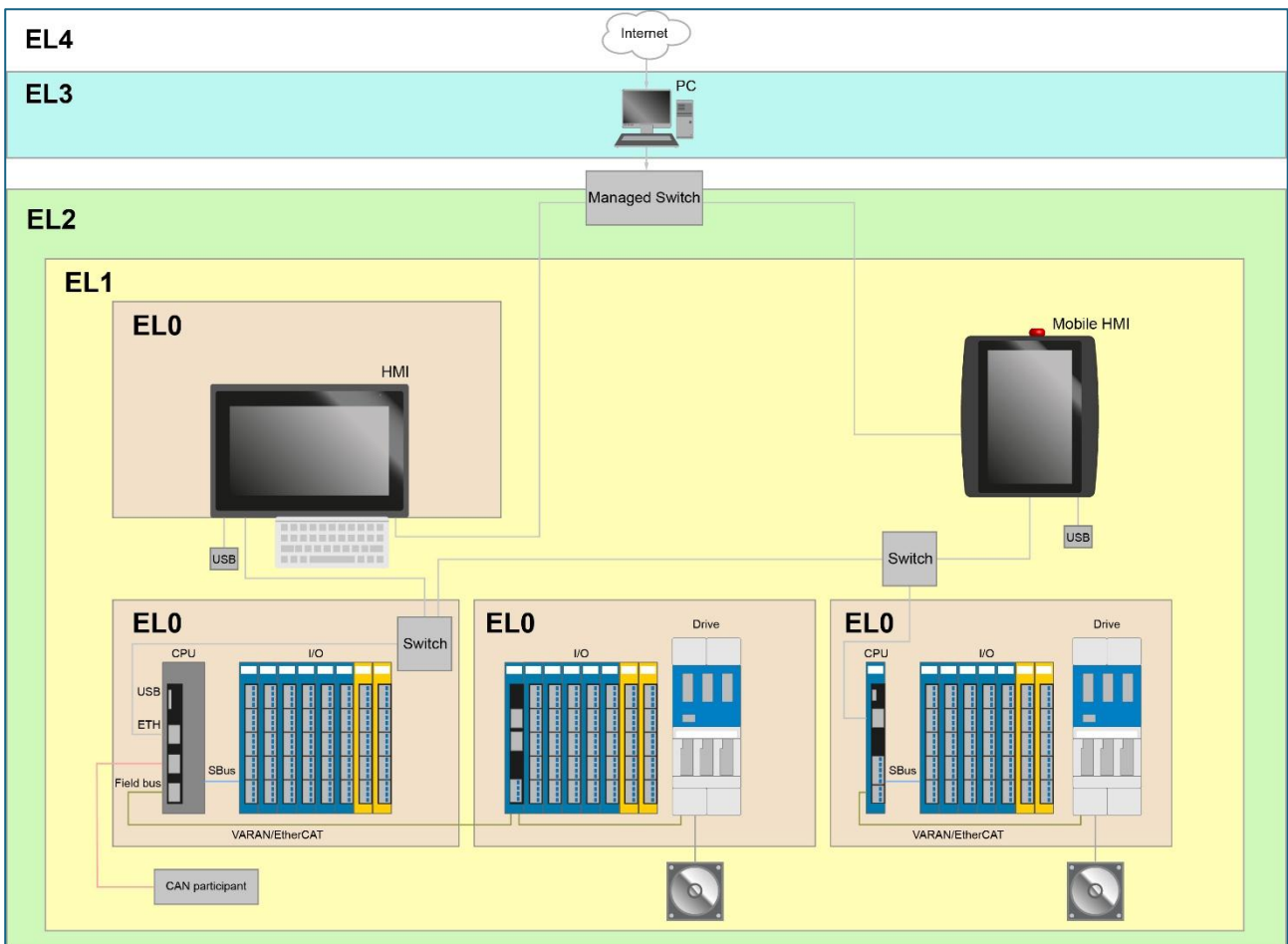
Im innersten Kern (EL0) befinden sich klassische PLCs und Steuerungskomponenten, die innerhalb eines geschlossenen Schaltschranks verbaut sind. Diese Komponenten sind primär durch physischen Schutz gegen Cyber-Angriffe abgesichert. Ein wesentliches Merkmal von EL0 ist, dass alle Kommunikationsschnittstellen ausschließlich innerhalb des Schaltschranks verlaufen.

Sobald eine Kommunikation über den Schaltschrank hinaus erfolgt – beispielsweise über einen Feldbus wie CAN – besteht zwar weiterhin physischer Schutz, jedoch entsteht eine externe Kommunikationsbeziehung. Die betroffenen Komponenten werden damit funktional dem Exposure Level 1 zugeordnet.

EL1 umfasst Geräte, deren cyber-exponierte Schnittstellen von außen zugänglich sind. Typische Beispiele sind HMIs, Einbauterminale oder Tragarmterminale. Auch wenn die Elektronik eines Einbauterminale und deren Schnittstellen innerhalb der Maschine oder des Schaltschranks verbaut sind, stellen Bedienelemente wie virtuelle Displays oder zugängliche USB-Schnittstellen eine Kommunikationsschnittstelle nach außen dar. Diese Schnittstellen sind somit einer erhöhten Cyber-Exponiertheit ausgesetzt und EL1 zuzuordnen.

EL2 repräsentiert ein segmentiertes OT-Netzwerk innerhalb der Produktionsanlage. Es bildet die kontrollierte und technisch abgesicherte Kommunikationsschicht, über die eine sichere Verbindung zum übergeordneten OT-Netz (EL3) hergestellt wird. Diese Kommunikationsbeziehung wird typischerweise durch sogenannte „Managed Switches“ realisiert, die neben der reinen Datenübertragung auch integrierte Cybersecurity-Mechanismen wie Netzwerksegmentierung, Zugriffskontrolle und Monitoring bereitstellen und damit eine kontrollierte und abgesicherte Kopplung zwischen den Netzen ermöglichen.

Das Exposure Level 3 beschreibt das OT-Netz der Fabrik. Jegliche Kommunikationsverbindung aus diesem Bereich in öffentliche Netze (Internet) muss zusätzlich über geeignete Firewalls und Sicherheitsmechanismen abgesichert sein, um unkontrollierte Zugriffe zu verhindern.



- EL0 => Schaltschrank, Komponenten verbaut in die Maschine/Anlage
- EL1 => Maschine/Anlage
- EL2 => Segmentiertes OT-Netz
- EL3 => IT-Netz der Fabrik
- EL4 => öffentliches Netz (Internet)

Die Grafik verdeutlicht, dass Security Assets abhängig von ihrer Einbindung und ihren Kommunikationsbeziehungen unterschiedlichen Exposure Levels zugeordnet werden können. Dabei ist jede Schnittstelle eines Assets separat hinsichtlich ihrer Cyber-Exponiertheit zu analysieren, da sich Sicherheitsrisiken nicht aus dem Produkt selbst, sondern aus der jeweiligen Kommunikationsbeziehung und Einbettung in die Systemarchitektur ergeben.

Dies wird insbesondere am Beispiel des Einbauterminals deutlich. Während die interne Elektronik einschließlich ihrer Kommunikationsschnittstellen dem Exposure Level EL0 zugeordnet ist, bildet das Display mit virtueller Tastatur ein bedienerseitiges Interface, das als EL1-Schnittstelle zu betrachten ist.

Wirksame Cybersecurity-Maßnahmen entstehen daher nicht allein auf Feldbus- oder Protokollebene, sondern maßgeblich durch architektonische Maßnahmen, gezielte Netzwerksegmentierung sowie klar definierte und kontrollierte Übergänge zwischen Sicherheitszonen.

6.3 Zusammenhang zwischen Exposure Level und erforderlichen Security-Maßnahmen

Die Einstufung eines Security Assets in einen Exposure Level (EL0–EL3) dient als Brücke zwischen Risikoanalyse und Umsetzung. Aus der realen Exponiertheit werden angemessene, nachvollziehbare und verhältnismäßige Sicherheitsmaßnahmen abgeleitet. Mit steigendem Exposure Level nimmt die Angriffsfläche zu – folglich steigen die Anforderungen an Zugriffskontrolle, Kommunikationssicherheit, Systemhärtung und Überwachung.

Grundprinzip: „Schutzbedarf folgt Exposure“

Sicherheitsmaßnahmen sollen so gewählt werden, dass sie:

- die realen Zugriffspfade (physisch, lokal, OT-weit, öffentlich) adressieren
- Trust Boundaries eindeutig definieren (wo beginnt/endet Vertrauen?)
- Komplexität nur dort erhöhen, wo sie einen Sicherheitsgewinn liefert

Ein Sonderfall in der OT ist die Kommunikation über Echtzeit-Feldbusse (z. B. EtherCAT/VARAN/CAN). Diese sind typischerweise nicht verschlüsselt, weshalb deren Schutz in niedrigen Exposure Levels primär über Architekturmaßnahmen (Segmentierung/Isolation) erfolgt. Ab höheren Exposure Levels muss die Sicherheitswirkung über gesicherte Übergänge und kontrollierte Kommunikationsgrenzen hergestellt werden – zum Beispiel über Remote Access Router, RAR 2400, RAR 2405, RAR 2410 usw. (siehe [SIGMATEK Homepage](#)).

Nicht nur Komponenten, sondern insbesondere Kommunikationspfade werden bewertet. Jede Verbindung über eine Trust Boundary erhöht den Schutzbedarf. Daraus folgt:

- Feldbussegmente bleiben (bis EL2) innerhalb eines geschützten Vertrauensbereichs.
- Ab EL3 müssen Übergänge aus dem Produktionsnetz in Richtung Maschine kontrolliert (z.B. über VPN), protokolliert (z.B. durch Logging) und kryptografisch abgesichert werden.
- In EL4 sind zusätzlich durchgängige Identität, Integrität und Authentizität für Kommunikation, Software und Updates zwingend.

Mit steigender Cyber-Exponiertheit reichen präventive Sicherheitsmaßnahmen allein nicht mehr aus. Es werden zusätzlich Maßnahmen zur Erkennung und Reaktion erforderlich. Dazu zählt insbesondere ein systematisches Schwachstellenmanagement (Vulnerability Management), das eine kontinuierliche Bewertung, Behandlung und Nachverfolgung von Sicherheitslücken über den Lebenszyklus ermöglicht.

Diese Sicherheitswirkung wird bei SIGMATEK im Kontext der aktuellen Salamander-Betriebssystemplattform mit integrierter Security-Architektur umgesetzt und unterstützt.

Frühere Betriebssysteme ohne systemseitig integrierte Security-Funktionen unterstützen hingegen kein Schwachstellenmanagement auf Betriebssystemebene. Ihr Einsatz ist daher auf Anwendungen mit niedriger Cyber-Exponiertheit beschränkt bzw. erfordert zusätzliche, architekturseitige Schutzmaßnahmen außerhalb des Betriebssystems. Die Abgrenzung, welche Betriebssystem-Versionen eine integrierte Security-Architektur unterstützen und welche als Legacy-S-Betriebssysteme einzuordnen sind, wird in Kapitel 7.3 näher erläutert.

7 Umsetzungs-Strategie des Sicherheitskonzeptes

Dieses Kapitel beschreibt, wie die abgeleiteten Sicherheitsziele in der Praxis umgesetzt werden. Der Fokus liegt auf Entwicklungsprozessen, sicherem Produktdesign, der sicheren Integration in Kundenumgebungen, dem Produktschutz über den Lebenszyklus sowie dem Sicherheitsbewusstsein entlang der Lieferkette. Damit wird ein konsistenter Rahmen geschaffen, der sowohl präventive als auch detektive und reaktive Maßnahmen umfasst.

7.1 Sichere Entwicklungsprozesse zur systematischen Vermeidung von Schwachstellen

SIGMATEK etabliert sichere Entwicklungsprozesse, um Schwachstellen bereits während der Entwicklung eines Produkts systematisch zu vermeiden und orientiert sich dabei an bewährte Sicherheitsstandards, insbesondere an der IEC 62443-4-1.

Ziel ist es, Sicherheitsanforderungen durchgängig zu berücksichtigen – von der Anforderungsdefinition über Design und Implementierung bis zu Verifikation, Release und Maintenance.

Dies umfasst:

- **Bedrohungsmodellierung:** Bereits in der frühen Entwicklungsphase werden potenzielle Sicherheitsrisiken und Schwachstellen durch Bedrohungsmodellierung und Risikobewertungen systematisch identifiziert werden.
- **Sicherheitsprüfungen:** Durch regelmäßige Code-Reviews und automatisierte statische Codeanalysen, werden in der Softwareentwicklung aktiv Schwachstellen vermieden. Automatisiert wird die Software auf bekannte Schwachstellen geprüft.
- **Entwicklungsrichtlinien:** Die Implementierung von Best Practices in der Softwareentwicklung, z.B. Input-Validierung, Buffer Overflow Schutz und Eingeschränkte Rechte für Programme und Benutzer.
- Definierter **Schwachstellenprozess** (Meldung, Bewertung, Behebung, Kommunikation, Traceability)

7.2 Security by Design und Security by Default

Security by Design bedeutet, dass Sicherheitsmechanismen bereits bei Architektur und Design der Komponenten berücksichtigt werden, anstatt sie nachträglich aufzusetzen. Security by Default stellt sicher, dass Produkte mit einer Basiskonfiguration ausgeliefert werden, die ein angemessenes Sicherheitsniveau unterstützt und Fehlkonfigurationen minimiert.

- **Security by Design:**
 - SIGMATEK verfolgt den Ansatz Security by Design, bei dem Security-Funktionen frühzeitig im Design- und Architekturkonzept adressiert werden sollen.
 - Kommunikationsbeziehungen sollen so konzipiert werden, dass sie standardmäßig in einem sicheren Modus betrieben werden.
- **Security by Default:**
 - Vorkonfigurierte, sichere Grundeinstellungen (z.B. restriktive Standardfreigaben, Minimierung offener Dienste) Prinzip „least privilege“: Berechtigungen sind initial begrenzt und müssen aktiv erweitert werden.
 - Alle SIGMATEK-Produkte werden mit einstellbaren Sicherheitsoptionen ausgeliefert, wie z.B. passwortgeschützte Admin-Zugänge, die auf sicheren Zugriffsmechanismen basieren.

Sicherheitsfunktionen sind nicht nur vorhanden, sondern wirksam, weil sie im Design vorgesehen und im Auslieferungszustand sinnvoll voreingestellt sind.

7.3 Rolle des Betriebssystems in der Sicherheitsarchitektur von Automatisierungskomponenten

Das Betriebssystem bildet die sicherheitstechnische Basis jeder Automatisierungskomponente. Es steuert Start- und Update-Prozesse, verwaltet Benutzer- und Berechtigungsmodelle, stellt Kommunikationsdienste bereit und definiert damit maßgeblich, welche Angriffsfläche ein Gerät überhaupt bietet.

In der Praxis ist die Cyber-Exponiertheit einer CPU oder eines HMI's daher nicht allein durch die Netzwerkanbindung bestimmt, sondern in hohem Maß durch die Fähigkeit des Betriebssystems, Zugriffe zu kontrollieren, Kommunikation abzusichern und Manipulationen an Software und Konfiguration zu verhindern.

Mit steigenden Exposure Levels verschiebt sich der Schwerpunkt der Absicherung. In niedrig exponierten Umgebungen kann die Sicherheitswirkung teilweise durch physische Schutzmaßnahmen und Netzwerksegmentierung („secure by environment“) erreicht werden. Ab höheren Exposure Levels genügt dieser Ansatz nicht mehr, da externe bzw. standortweite Kommunikationsbeziehungen nur dann beherrschbar sind, wenn das Endgerät selbst über integrierte Security-Mechanismen verfügt.

Dazu zählen insbesondere Secure Boot zur Sicherstellung der Integrität beim Systemstart, authentifizierte und integritätsgesicherte Updates sowie gehärtete, kryptografisch abgesicherte Kommunikationsschnittstellen.

Bei SIGMATEK unterscheidet sich der verfügbare Security-Funktionsumfang in Abhängigkeit von der eingesetzten S-Betriebssystemversion.

Dabei werden folgende Release-Stände unterschieden:

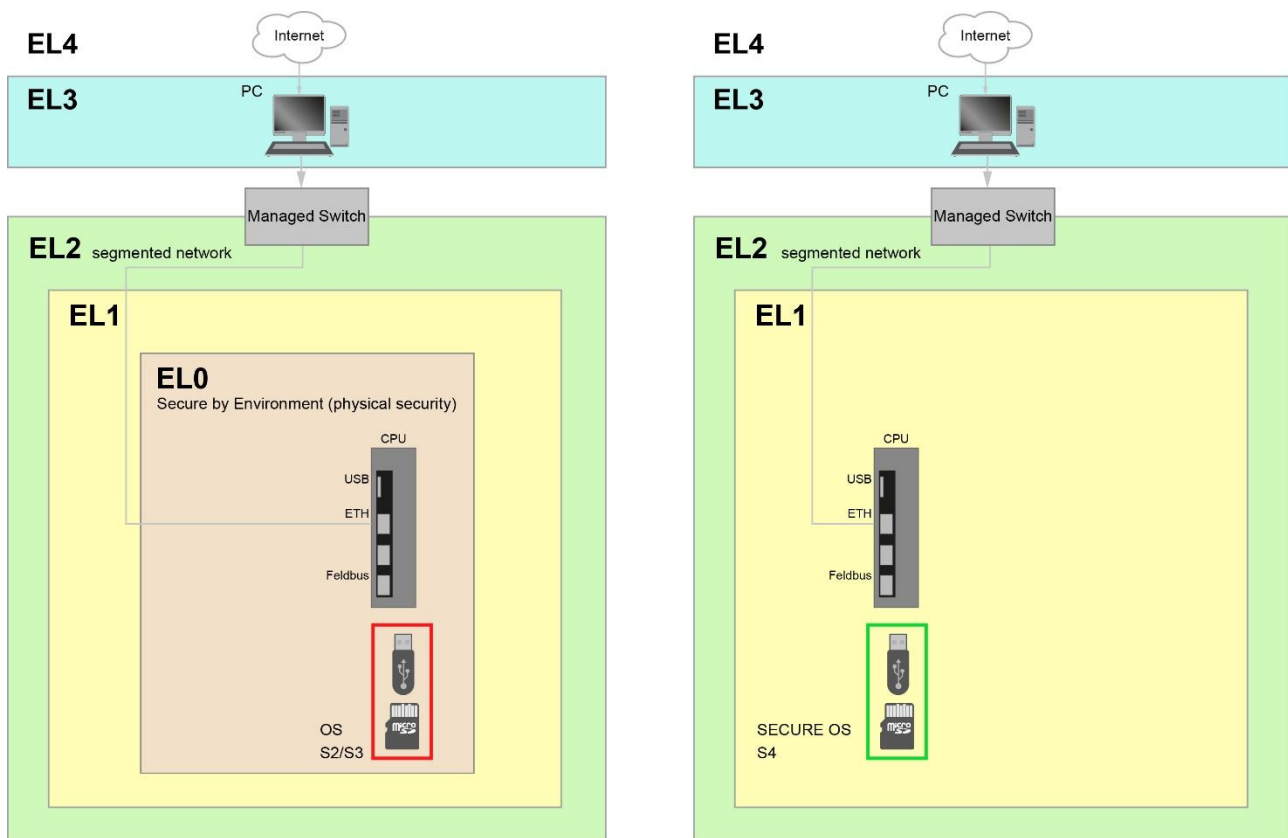
- S2-Betriebssysteme der Versionen 09.01.xxx und 09.02.xxx
- S3-Betriebssysteme der Versionen 09.03.xxx und 09.04.xxx
- S4-Betriebssysteme ab Version 09.07.xxx

S2 und S3 wurden primär für funktionale Anforderungen in geschlossenen Automatisierungsumgebungen entwickelt und verfügen über eine eingeschränkte integrierte Security-Architektur. Diese Versionen werden auch als Legacy-Betriebssysteme bezeichnet.

S4-Betriebssysteme ab Release 09.07.xxx werden hingegen gezielt weiterentwickelt und um systemseitige Security-Funktionen erweitert. Diese bilden die Grundlage für eine integrierte Absicherung der Automatisierungskomponente und werden im Folgenden als S4 bezeichnet.

Dieses Kapitel erläutert, wie unterschiedliche Betriebssystem-Ausprägungen den zulässigen Einsatzbereich von Automatisierungskomponenten von SIGMATEK bestimmen. Auf dieser Grundlage wird gezeigt, wie sich die Cyber-Exponiertheit nicht nur durch Umfeld- und Netzwerkkonzepte, sondern zunehmend durch systemseitige Sicherheitsfunktionen kontrollieren lässt.

Folgende Abbildung stellt zwei unterschiedliche Sicherheitsansätze für SIGMATEK-Steuerungssysteme gegenüber und zeigt, wie sich die Fähigkeiten des eingesetzten Betriebssystems direkt auf die zulässigen Exposure Levels (EL) und damit auf die Integrations- und Einsatzmöglichkeiten im Gesamtsystem auswirken.



Auf der linken Seite ist eine SIGMATEK-CPU mit dem Betriebssystem S2 oder S3 dargestellt. Wie bereits in vorherigen Kapiteln beschrieben, verfügen diese Betriebssysteme über eingeschränkte Cybersecurity-Funktionen. Der erforderliche Schutz dieser Systeme wird daher primär durch das Umfeld sichergestellt („secure by environment“):

- **Physische Schutzmaßnahmen** (geschlossener Schaltschrank, Zugang nur mit Schlüssel oder Werkzeug)
- **Begrenzung auf niedrige Exposure Levels** (EL0 / EL1)
- **Kommunikationsverbindung bis EL2**, sofern eine konsequente Netzwerksegmentierung implementiert ist und der erforderliche Cyberschutz dadurch auf Systemebene gewährleistet werden kann.
- **Nutzung externer Sicherheitskomponenten**, um höhere Exposure Levels architektonisch abzusichern

Bis einschließlich EL2 können die Geräte über Ethernet auch ohne kryptografisch gesicherte Kommunikation betrieben werden, sofern sie ausschließlich in abgegrenzten, vertrauenswürdigen Netzwerksegmenten eingesetzt werden.

Sobald jedoch Kommunikationsbeziehungen über EL2 hinaus erforderlich sind, kann der notwendige Schutz nicht mehr allein durch Netzwerksegmentierung erreicht werden. In diesen Fällen ist der Einsatz einer zusätzlichen externen Sicherheitskomponente, z.B. RAR 2410, erforderlich. Dieser stellt die kryptografische Absicherung, Authentisierung sowie kontrollierte Übergänge zwischen unterschiedlichen Netzwerkzonen sicher.

Damit sind S2 und S3 grundsätzlich auf Einsatzszenarien mit geringer bis moderater Cyber-Exponiertheit beschränkt, bei denen keine oder nur streng kontrollierte externe Kommunikationsbeziehungen bestehen.

Auf der rechten Seite zeigt die Grafik ein CPU mit S4 Betriebssystem, das Sicherheitsfunktionen direkt im Systemdesign verankert. Dadurch kann die Sicherheitswirkung nicht mehr ausschließlich über das Umfeld, sondern über integrierte technische Maßnahmen hergestellt werden.

Das sichere Betriebssystem erweitert den zulässigen Einsatzbereich von SIGMATEK Produkten gezielt auf höhere Exposure Levels (EL3 und EL4), abhängig von den genutzten Schnittstellen bzw. Diensten und unterstützt damit moderne OT und IT-nahe Architekturen.

Die Kern- Security-Funktionen des sicheren Betriebssystems gliedern sich in drei Hauptbereiche:

Secure Online Interface

(Netzwerk- und Kommunikationshärtung)

Das Secure Online Interface bündelt Maßnahmen zur Absicherung von Netzwerkkommunikation und Online-Zugängen, insbesondere:

- Default-Aktivierung moderner Verschlüsselung- und Authentifizierungsmechanismen für z.B. LASAL-Verbindungen
- Vorkonfigurierte Firewall-Restriktionen, z. B. Whitelist-basierte Kommunikationsfreigaben
- Optionale Vorinstallation einer integrierten VPN-Lösung

Diese Funktionen ermöglichen (vom jeweiligen Dienst abhängig) kontrollierte und abgesicherte Kommunikationsbeziehungen über Trust Boundaries hinweg und reduzieren die Angriffsfläche bei externer oder standortweiter Vernetzung.

Secure Update

(Authentizität von Software-Updates)

Der Secure Update Mechanismus stellt sicher, dass ausschließlich autorisierte Software-Updates auf die Steuerung installiert werden können. Dies wird durch geeignete kryptografische Verfahren, insbesondere durch digitale Signaturen und deren überprüfte Vertrauensanker, unterstützt.

Secure Boot *(Integrität)*

Secure Boot ist eine Schutzmaßnahme, die sicherstellt, dass beim Systemstart ausschließlich unveränderte, autorisierte Software geladen wird. Geschützt sind unter anderem:

- Bootloader
- Kernel
- Dateisystem
- Benutzerpartition

Insgesamt bilden Secure Online Interface, Secure Update und Secure Boot ein konsistentes Sicherheitsfundament, das zentrale Schutzziele wie Vertraulichkeit, Integrität und Authentizität systematisch adressiert und damit die Voraussetzung für den sicheren Betrieb von Automatisierungskomponenten in erhöhten Exposure Levels schafft.

7.4 Sichere Integration der SIGMATEK-Komponenten in heterogene Kundenumgebungen

- **Schutzmechanismen auf Kommunikations-, Zugriffs- und Betriebssystemebene:**

SIGMATEK-Komponenten wurden für die Einbindung in ein vor Fremdzugriff geschütztes Netzwerk sowie Installation in einem zugangsgeschützten Bereich entwickelt. Auf das Netzwerk oder die Umgebung können zum Beispiel Gefahren wie, unautorisierte Zugriff, Datenmanipulation, physikalische Zugriffe und Manipulation einwirken.

Es obliegt dem Maschinenhersteller oder Betreiber eine Risikoanalyse der Verbindungen zwischen SIGMATEK-Komponenten und der Integration in die Gesamtinfrastruktur durchzuführen.

Daraus können sich beispielsweise folgende Maßnahme ergeben: zugangsgeschützter Bereich, Deaktivierung von Ethernet-Diensten und automatischer Adressenvergabe, Firewalls, VPNs und IDS/IPS-Systeme (Intrusion Detection/Prevention Systeme), um eine sichere Kommunikation in einem sicherheitskritischen Netzwerk zu gewährleisten.

- **Trennung von Verantwortlichkeiten:**

- SIGMATEK (**Komponentenhersteller**) ist verantwortlich für die Bereitstellung sicherer Automatisierungskomponenten und Schnittstellen nach dem Prinzip *security by design und security by default*. Dazu gehört insbesondere die Umsetzung systemseitiger Sicherheitsmechanismen sowie die Bereitstellung notwendiger Sicherheitsupdates und -patches für die jeweilige Produktplattform.
- Der **Maschinenhersteller** übernimmt eine zentrale Rolle bei der Sicherstellung der Cybersecurity der Gesamtmaschine. In seinem Verantwortungsbereich liegen insbesondere folgende Aufgaben:
 - Der Maschinenhersteller definiert die Cyber-Exponiertheit der Maschine und legt fest, welche Schnittstellen, Dienste und Kommunikationsbeziehungen für den vorgesehenen Einsatz erforderlich und zulässig sind.
 - Durch die Entwicklung der kundenspezifischen Applikationssoftware bestimmt der Maschinenhersteller maßgeblich, welche systemseitig bereitgestellten Security-Funktionen genutzt, konfiguriert oder wirksam zur Anwendung kommen.
 - Der Maschinenhersteller stellt sicher, dass die Integration von Security-Updates und -Patches die funktionalen, sicherheitstechnischen und anwendungsspezifischen Anforderungen der Maschine nicht negativ beeinflusst.
 - Er ist zudem dafür verantwortlich, dass Security-Patches in geeigneter Form an den Betreiber weitergegeben werden, sodass diese im Rahmen des sicheren Betriebs umgesetzt werden können.

- Der **Betreiber** ist verantwortlich für den sicheren Betrieb der Maschine über ihren gesamten Lebenszyklus hinweg, basierend auf den vom Maschinenhersteller definierten Einsatzbedingungen und Exposure Levels.
- Der Betreiber stellt sicher, dass die Maschine ausschließlich innerhalb der vom Maschinenhersteller definierten Exposure Levels betrieben wird.
- Der Betreiber ist verantwortlich für die Umsetzung organisatorischer und technischer Betriebsmaßnahmen.
- Der Betreiber stellt den ordnungsgemäßen Umgang mit Security-Updates und -Patches sicher.

7.5 Produktschutz über den gesamten Lebenszyklus

Cybersecurity ist ein kontinuierlicher Prozess über den gesamten Produktlebenszyklus von der Auslieferung bis zum Ende der Nutzungsdauer. Neben präventiven Maßnahmen sind insbesondere Update- und Patchfähigkeit sowie der Umgang mit Bestandssystemen entscheidend.

- **Sichere Firmware-Updates und Patching-Mechanismen:**

SIGMATEK stellt dem Maschinenhersteller neue Betriebssystemversionen auf einem noch zu definierenden Portal zur Verfügung.

Die Durchführung und Verifikation von Updates liegen in der Verantwortung des Maschinenherstellers.

- **Schutzkonzepte für Alt- und Bestandssysteme:**

Legacy Produkte ohne Cybersecurity-Maßnahmen müssen von kritischen Netzwerken isoliert werden, um das Risiko einer Ausbreitung von Bedrohungen zu minimieren. Ein Legacy- Steuerungssystem könnte in einem eigenen Netzwerksegment laufen, getrennt von den anderen modernen Systemen, um zu verhindern, dass es als Einstiegspunkt für Angriffe auf andere Systeme dient.

- **Abschottung durch physische Sicherheit:**

Bei kritischen Legacy-Systemen, die keine modernen Sicherheitsmechanismen bieten, muss der Maschinenhersteller physische Sicherheitsvorkehrungen treffen. Dies umfasst den Zugangsschutz zu den Geräten selbst und die Sicherstellung, dass nur autorisierte Personen physischen Zugang zu den Geräten haben.

7.6 Voraussetzungen und Grenzen der Update- und Migrationsfähigkeit

Die Möglichkeit, ein bestehendes Betriebssystem auf ein Betriebssystem mit integrierten Sicherheitsfunktionen zu aktualisieren, hängt wesentlich von den Eigenschaften der eingesetzten Hardware-Plattform ab.

Insbesondere integrierte Cybersecurity-Funktionen wie Secure Boot, kryptografisch abgesicherte Kommunikation, sowie die Authentifizierung und Integrität von Software-Updates setzen entsprechende Systemressourcen und hardwareseitige Sicherheitsmechanismen voraus.

Ein Upgrade ist daher ausschließlich auf Geräten möglich, auf denen bereits S4 eingesetzt wird. Mit dem Einsatz von S4 ist sichergestellt, dass die jeweilige Hardware-Plattform über die notwendigen Rechen-, Speicher- und Sicherheitsressourcen verfügt, um die erweiterten Security-Funktionen zuverlässig umzusetzen.

Demgegenüber ist ein Upgrade auf S4 bei Geräten mit S2 oder S3 nicht möglich. Diese Betriebssysteme kommen auf älteren Hardware-Plattformen (z.B. EDGE2-Technologie) zum Einsatz, die die erforderlichen technischen Voraussetzungen für moderne Cyber-Security Mechanismen nicht bereitstellen.

In solchen Fällen kann der erforderliche (Cyber-)Schutz nicht durch ein Software-Upgrade erreicht werden.

Stattdessen müssen kompensierende Maßnahmen auf System- und Architekturebene umgesetzt werden, wie in den vorherigen Kapiteln beschrieben, durch konsequente Netzwerksegmentierung, physische Zugriffsbeschränkungen sowie den Einsatz externer Sicherheitskomponenten.

Die Updatefähigkeit auf S4 ist damit kein generelles Software-Feature, sondern eine hardwareabhängige Systemeigenschaft, die bereits bei der Auswahl der Plattform und der vorgesehenen Exposure-Level-Einstufung berücksichtigt werden muss.

8 Zusammenfassung

Die zunehmende Vernetzung und Digitalisierung industrieller Produktionssysteme erfordert ein ganzheitliches Verständnis von Cybersicherheit. SIGMATEK begegnet dieser Entwicklung mit einem umfassenden Sicherheitskonzept, das darauf abzielt, Automatisierungskomponenten von Beginn an gegen Cyberbedrohungen abzusichern.

Dabei steht die Integration von Sicherheitsmaßnahmen über den gesamten Produktlebenszyklus hinweg im Mittelpunkt – von der ersten Spezifikation über die Entwicklung und Fertigung bis hin zum langfristigen Support.

Im Zentrum des Konzepts steht die konsequente Umsetzung sicherer Entwicklungsprozesse, die sich an etablierten Normen orientieren. Eine zentrale methodische Grundlage ist die Bewertung der Cyber-Exponiertheit über Exposure Levels (EL0–EL4). Diese Betrachtung erfolgt nicht nur auf Maschinenebene, sondern pro Security Asset und pro Kommunikationsbeziehung. Sicherheitsrisiken ergeben sich aus der Einbettung in die Systemarchitektur und den tatsächlich genutzten Schnittstellen und Diensten. Wirksame Cybersecurity entsteht im Zusammenspiel aus Architekturmaßnahmen (Segmentierung, kontrollierte Übergänge), systemseitigen Schutzfunktionen (Zugriffskontrolle, Härtung, Kryptografie) sowie detektiven und reaktiven Maßnahmen (z. B. Schwachstellenmanagement).

Bereits in der Entwurfsphase werden potenzielle Schwachstellen identifiziert und durch geeignete Maßnahmen adressiert. Sicherheitsmechanismen werden von Anfang an in die Produkte integriert und standardmäßig aktiviert, ohne dabei die Echtzeitfähigkeit oder funktionale Sicherheit der Systeme zu beeinträchtigen.

Ein weiterer Schwerpunkt liegt auf der sicheren Einbindung der SIGMATEK-Komponenten in unterschiedlichste Kundenumgebungen. Dies erfordert sowohl technische Schutzmaßnahmen auf Kommunikations- und Betriebssystemebene als auch eine klare Trennung der Verantwortlichkeiten zwischen Komponentenhersteller, Maschinenbauer und Betreiber. Auch nach der Inbetriebnahme wird der Schutz der Produkte durch sichere Update-Mechanismen und Konzepte für den Umgang mit Alt- und Bestandssystemen gewährleistet.

Darüber hinaus fördert SIGMATEK aktiv das Sicherheitsbewusstsein entlang der gesamten Lieferkette.

Mit diesem ganzheitlichen Ansatz leistet SIGMATEK einen entscheidenden Beitrag zur Absicherung moderner Produktionssysteme und stärkt das Vertrauen seiner Kunden in die digitale Transformation der Industrie.

SIGMATEK wird die Weiterentwicklung des Sicherheitskonzeptes kontinuierlich an neue Bedrohungslagen und technologische Trends anpassen.

Das Ziel bleibt dabei konstant: Automation "Made by SIGMATEK" dauerhaft sicher und zukunftsfähig zu gestalten.

Änderungen der Dokumentation

Änderungsdatum	Betroffene Seite(n)	Kapitel	Vermerk	Version
20.10.2025		Alle		1.0
09.04.2026		3, 6, 7	Kap.3: Europäischer Rechts- und Normenrahmen für Cybersecurity Kap.6: Risikoanalyse und Bewertung der Cyber-Exponiertheit Kap.7: 7.3 Rolle des Betriebssystems in der Sicherheitsarchitektur von Automatisierungskomponenten 7.6 Voraussetzungen und Grenzen der Update- und Migrationsfähigkeit	2.0