PHYSEC
SECURITY FOR THINGS

IEC 62443: Why physical protection is indispensable in OT security

Industrial facilities and critical infrastructures are increasingly becoming the focus of cyber attacks. However, traditional IT security measures alone are not enough to reliably protect complex industrial systems. This is precisely where the IEC 62443 series of standards comes in: It provides a comprehensive framework for cyber security in industrial automation and control systems (IACS).

While most people initially focus on firewalls, access rights or encryption, a look at the standard shows that physical protection also plays a key role. This article provides a structured guide to IEC 62443, explains key security principles and finally focuses on physical protection in OT environments, which is often underestimated but required by the standard.

IEC 62443 was developed to protect industrial networks, systems and components against threats - regardless of whether these arise from cyberspace, operational errors or physical interference. Unlike purely IT-oriented security standards, IEC 62443 takes into account the special conditions in industrial automation: long life cycles, heterogeneous systems, real-time processing and often open physical access options.

All relevant stakeholders are addressed: manufacturers (m), who develop safe components; system integrators (i), who design complete systems; and operators (o), who assume responsibility for safe operation.

Own illustration, based on: Quick Start Guide: An Overview of ISA/IEC 62443 Standards, ISA Global Cybersecurity Alliance

The four main areas of IEC 62443

IEC 62443 has a modular structure and is divided into four large sections that build on each other. Each part takes a different perspective on the topic of safety and is aimed at different areas of responsibility.

62443-1: lays the conceptual foundation. It introduces key models such as 'Defence in Depth', as well as basic definitions and terms relating to industrial cyber security. This standardised language is necessary so that everyone involved - from development to system integration and operation - shares a common understanding. Physical protection is not yet covered in detail in this section but is clearly positioned as a level of protection in the security model.

62443-2: deals with security management at an organisational level. Among other things, it requires an information security management system (ISMS) with defined processes for risk analyses, vulnerability management and continuous improvement. Aspects such as access regulations, physical access guidelines and organisational responsibilities for physical security measures are also part of the normative expectation here.

62443-3: focusses on the system level. This deals with the security architecture of complete OT systems, from network segmentation and access controls to the assignment of security levels. This section is particularly relevant when it comes to the practical implementation of physical security: access control, securing zone boundaries and protecting communication paths are explicitly required here.

62443-4: addresses the technical implementation at component level. This section is aimed in particular at manufacturers and requires devices to be tamper-resistant, securely configurable and verifiable. Physical security is particularly evident here in the form of tamper detection, housing protection or protection against unauthorised access to service interfaces.

The BSI uses a clear table to illustrate the individual sub-standards within the four areas of IEC 62443, which topics they cover, and which roles are addressed. The sub-standards marked with an asterisk are particularly specific regarding the requirements for physical security.

Topic	Sub-Standard	Role
Basic concepts, models and terms for the security of industrial automation systems	IEC 62443-1-1 bis IEC 62443-1-4	m, i, o
Requirements for an IT security programme for IACS operators	IEC 62443-2-1	o
Methodology for assessing the protection of industrial automation systems in operation	IEC 62443-2-2	o
Patch management in IACS environments	IEC 62443-2-3	o, m
Security requirements for service providers for industrial automation systems	IEC 62443-2-4	i
Security requirements at network level	IEC 62443-3-1*	i, o
Security risk assessment for system design	IEC 62443-3-2	o
Security requirements at system level	IEC 62443-3-3*	m, o
Development process	IEC 62443-4-1*	m
Product capabilities	IEC 62443-4-2*	m

Source: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile

With these areas, the standard offers a consistent security architecture (conceptual, organisational, systemic and technical). However, in order to understand how these levels interact, it is worth looking at two central principles of the standard.

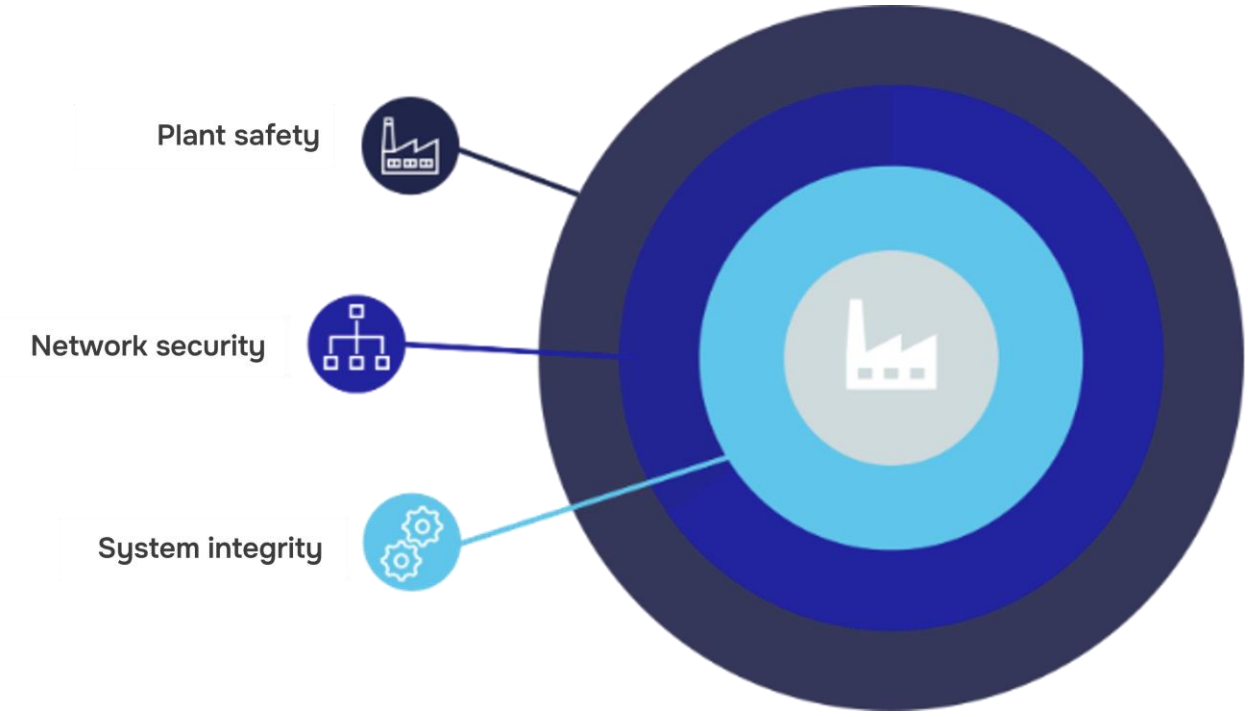
Defence in Depth

A core principle of IEC 62443 is the 'Defence in Depth' model. Security is not conceived as a single measure, but as a multi-layered defence consisting of complementary layers. Each of these layers should remain effective even if another fails.

It is crucial that these layers are not only of a technical nature. They are also distributed along the lines of responsibility:

- Manufacturers ensure that devices are tamper-resistant ex works through security features such as secure firmware, disabled debug ports or housing protection.
- System integrators plan how these devices are embedded in secure zones, how communication connections are secured and how access points are controlled.
- Operators are organisationally and technically responsible for ongoing protection during operation, for example by monitoring access, alarm responses or status checks.

This creates an interlocking system of responsibility and protection mechanisms that considers both digital and physical attack vectors.



Safety zones and conduits

Another central principle of the standard is the subdivision of industrial systems into safety zones and conduits. Zones are groups of systems with similar safety requirements, such as process control systems, field devices or engineering stations. Conduits are defined communication paths between these zones that must be controlled and secured.

This logical segmentation is not only crucial from a network perspective, but also for physical security. Because each zone can and must be physically secured: Who is allowed access? Which doors are locked? Which enclosures are sealed? In practice, conduits must also be protected against physical manipulation such as eavesdropping or interruption of communication paths. Physical protection is therefore not downstream but firmly embedded in the security architecture.

The four security levels of IEC 62443

IEC 62443 defines security levels (SL) that can be used to assess and implement the necessary level of protection for industrial systems, components and networks. They are used for the risk-orientated classification of the threats that a system must withstand. The standard distinguishes between a total of four security levels, which build on each other in a staggered manner.

SL 1 - Protection against unintentional incidents

SL1 is the minimum level that should be implemented in almost every OT environment. It corresponds to a basic level of security precautions.

- **Threat scenario:** Random or unintentional events (e.g. incorrect operation, system errors)
- **Attacker profile:** No targeted attacker
- **Objective:** Basic protection against accidental system compromise

SL 2 - Protection against simple attacks with limited means

SL2 is often required in industrial networks with an increased risk of exposure, e.g. if service personnel or external service providers have regular access.

- **Threat scenario:** Attacks by technically unskilled actors with generally accessible means
- **Attacker profile:** Low level of expertise, low motivation, simple tools
- **Goal:** Preventing attacks by opportunists or insiders with limited access

SL 3 - Protection against targeted attacks with specialised knowledge

SL3 is required in critical environments where there is a threat of targeted attacks on automation processes or systems with high economic or security-relevant value.

- **Threat scenario:** Targeted attacks on the OT infrastructure
- **Attacker profile:** IACS-specific expertise, medium resources, targeted approach
- **Objective:** Protection against actors with a professional background, such as hacktivists or industrial espionage

SL 4 - Protection against highly professional attacks with extensive resources

SL4 is relevant for operators of critical infrastructures, particularly in the energy, water, transport, health and defence sectors. It requires a comprehensive security architecture - both technically and organisationally.

- **Threat scenario:** State-sponsored attacks, APTs, strategic sabotage
- **Attacker profile:** Very high motivation, extensive resources, in-depth IACS expertise
- **Goal:** Maximum resilience to complex and targeted cyber attacks

Definition of Security Levels (SL)

Security Level	Definition	Means / attack tools	Resources	Skills	Motivation
1	Protection against incidental or accidental offences	-	-	-	-
2	Protection against intentional injury with simple means, limited resources, general skills and low motivation	Easy	Low	Generic	Low
3	Protection against intentional offences with sophisticated means, moderate resources, IACS-specific skills and moderate motivation	Sophisticated	Medium	IACS-specific	Medium
4	Protection against intentional offences with sophisticated means, extended resources, IACS-specific skills and high motivation	Sophisticated	Extended	IACS-specific	High

Source: https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

Physical security requirements

Physical security is a consistent cross-cutting topic in IEC 62443. It begins with higher-level concepts such as defence in depth and zoning via zones and conduits, is specified in organisational requirements, taken into account in the system architecture and technically implemented at device level. In the technical parts of the standard - in particular IEC 62443-3-3 and IEC 62443-4-2 - clear requirements are derived from this: for example, for access control, enclosure protection, tamper detection, interface hardening and the verifiable integrity of devices.

The aim of all these measures is verifiable device and system integrity. The security of the entire OT infrastructure can only be guaranteed if an asset is considered unchanged, trustworthy and authentic. The security of the entire OT infrastructure can only be guaranteed if an asset is considered unchanged, trustworthy and authentic. The physical components are often the weakest link, especially in the context of closed access operations (CAO). CAOs refer to cyber operations that require physical or local access to the system or are deliberately created using covert methods, for example via manipulated supply chains or compromised hardware components. Unlike remote access operations (ROA) via wide area networks, CAOs often remain invisible to traditional IT security systems.

Examples of closed-access attacks:

- **'Evil Maid' attacks:** An attacker manipulates a device that is left unattended, for example by introducing a keylogger at firmware level.
- **Firmware manipulation**: Devices in the supply chain are compromised before use. The attack is 'closed' as it does not require a network connection.

Various measures are used to prevent such attacks and ensure integrity:

- **Physical access control:** the first protection mechanism is controlled access. Only authorised persons may gain access to critical devices or areas. Card readers, biometric systems, lockable technical rooms, video surveillance and visitor management are typically used for this purpose.
- **Tamper protection:** Devices and interfaces such as JTAG, UART or debug ports are protected against unauthorised access by sensors and physical isolation. Tampering attempts such as housing openings or physical attacks are recognised, alerted and logged.
- **System and device hardening:** Devices must be hardened and protected against physically initiated misconduct, e.g. by deactivating unused ports and functions, secure booting / secure initialisation and cryptographic authentication.

Traditional protective measures are often complex, cost-intensive or technically demanding to implement. This is precisely where PHYSEC SEAL comes in: With SEAL, the integrity of physical assets can be verified in a hardware-supported, tamper-proof and automated manner. This allows existing protective measures to be supplemented or even relieved in a targeted manner, making the entire security architecture more economical and scalable.
How PHYSEC SEAL specifically contributes to the implementation of IEC 62443

How PHYSEC SEAL specifically contributes to the implementation of IEC 62443

A central objective of IEC 62443 is to systematically secure both digital and physical attack vectors. Particularly in an industrial environment, targeted manipulation at hardware level poses a real threat, often using frighteningly simple means. One prominent example is the USB Rubber Ducky. This is a device that looks like an ordinary USB stick, but when plugged in pretends to be a keyboard and automatically executes pre-programmed commands at high speed on the target system, e.g. to open a command line window, download malicious code or compromise user accounts.

Such tools are often used by penetration testers, but also by attackers, to gain access to systems in just a few seconds. There are also modified USB cables with a WLAN module that enable remote access to connected systems - while appearing completely normal on the outside. Even more sophisticated are hardware implants from the NSA's leaked ANT catalogue. One example: COTTONMOUTH-I, a USB plug with a built-in radio transmitter that can intercept keystrokes and receive commands completely camouflaged in the housing of a USB cable. Modified network cards or keyboards with eavesdropping modules are also part of the arsenal of such espionage tools.

These real threats show why IEC 62443 sees physical security as an essential part of 'Defence in Depth'. PHYSEC SEAL makes a measurable contribution, particularly in the areas of system integrity, incident response and availability, as well as to specific technical requirements for components. SEAL can therefore make a concrete contribution to the fulfilment of 3 out of 7 Foundational Requirements and indirectly contribute to many other requirements.

Contribution to the Foundational Requirements (FR):

- **FR 3 - System Integrity:** SEAL monitors the physical integrity of devices, housings and interfaces and recognises tamper protection in real time. SEAL therefore fulfils the requirements for maintaining system integrity at all security levels (SL1-SL4). Particularly at the higher levels, which specifically address resource-intensive attackers, tamper-proof status monitoring by SEAL is a critical element.

- **FR6 - Timely Response to Events:** SEAL recognises physical security events and automatically forwards messages to higher-level systems or recipients. This immediate response supports efficient incident response management, which is a must for security levels SL2 - SL4.

- **FR7 - Resource Availability:** By detecting sabotage or physical access at an early stage, SEAL protects industrial systems from consequential damage such as operational interruptions or failures. This not only ensures availability in accordance with the standard, but also significantly reduces response times in an emergency.

Fulfilment of technical requirements from IEC 62443-4-2:

- SEAL fulfils the highest security requirements (SL4) for embedded devices, network devices and host systems (EDR / NDR / HDR 3.11 - Physical tamper resistance and detection), because tampering is detected, an alarm is sent to defined recipients and the results are logged seamlessly and tamper-proof.

- SEAL is continuously active, recognises security-relevant physical events and can be connected to SIEM or monitoring systems. SEAL is therefore able to fulfil the requirements for continuous monitoring on SL4 (CR 6.2 - Continuous Monitoring).

- SEAL can reliably act as an initial trigger for the activation of active protection mechanisms such as ‘Fail Close’ or ‘Island Mode’. In integrations with manufacturers, SEAL can thus enable manipulation-based transitions to secure operating modes (NDR 5.2 - Zone Boundary Protection).

- SEAL indirectly contributes to integrity assurance within the boot process through status monitoring - especially if manipulations occur before or during startup (CR 3.14 - Boot Process Integrity).

SEAL is a standard-compliant, physically based module for safeguarding industrial systems. SEAL thus demonstrably supports companies in fulfilling regulatory requirements from IEC 62443 and at the same time increases operational resilience in OT.

Schedule your expert consultation and strengthen your IEC 62443 compliance!