Author: Carsten Bokholt
November 2025

WHITEPAPER

INDUSTRIAL SECURITY

TRUST THROUGH SECURITY – HOW HELMHOLZ PROTECTS INDUSTRIAL COMMUNICATIONS.

A guide for manufacturers and operators of machinery on how to comply with current EU legislation.

www.helmholz.com

Helmholz®
COMPATIBLE WITH YOU

TABLE OF CONTENTS

ABOUT US

Where machines communicate, Helmholz builds trust: with technology that connects, protects, and simply makes industrial communication secure.

For over 35 years, Helmholz has been developing solutions that make industrial networks more efficient and future-proof – from the field level to the cloud. As a specialist in PROFINET, Industrial Ethernet, and IoT, Helmholz focuses on quality, precision, and partnership-based thinking.

Secure communication – from components to systems

Our goal: to make technology understandable and security a matter of course. Whether PROFINET, Industrial Ethernet, or IoT – Helmholz offers the right components for smooth communication in industrial plants.

From switches and gateways to firewalls and remote access solutions, we create systems that connect, protect, and make processes more efficient. All products are developed, tested, and manufactured in Germany in accordance with DIN ISO 9001:2015 – for quality you can rely on.

Helmholz takes automation one step further: with security by design, open standards, and solutions that meet the increasing demands of industrial security.

In this way, we support machine builders, integrators, and operators in networking their systems reliably, scalably, and in compliance with standards.

Helmholz – Compatible with you. Because genuine partnership is the basis for secure communication.

MOTIVATION & VISION

The security of machines and systems is crucial for a stable and fail-safe production process. Only those who secure their communications can ensure that their systems are permanently available.

With new regulations such as the Cyber Resilience Act (CRA) and the European Machinery Regulation, appropriate cybersecurity measures are now mandatory for anyone who places products or machines on the market.

Motivation

At Helmholz, security was considered early on in the company and in its products. This document is intended to provide an overview of the legal situation and the relevant standards for manufacturers, machine builders, and end users, and to give an update and outlook on implementation at Helmholz.

Vision

Trust through security! Security is more than just technology – it's an attitude. Helmholz integrates security by design into every product to provide lasting protection for industrial communication.

Our vision: Trust arises where security begins.

RELEVANT REGULATIONS AND GUIDELINES

With the triumph of Ethernet networking in manufacturing plants, cybersecurity is also gaining central importance, as current standards and guidelines show.

The EU legislator has drafted or updated various regulations and directives on this topic. EU regulations are effective without national legislation, such as the Cyber Resilience Act (CRA). In contrast, EU directives must first be transposed into national legislation by EU countries, such as NIS2.

Cyber Resilience Act

The Cyber Resilience Act covers products (components) with digital elements. These can be cell phones, electronic toys with USB, washing machines with Wi-Fi, IT products, or even PLCs or industrial switches. It concerns the processing, storage, and transmission of digital data. This includes both hardware and software, including the cloud application associated with the product.

The CRA will become mandatory for all products sold from December 2027 onwards. However, there are exceptions to the CRA. These include industries that are already regulated (automotive, medical, aeronautics), open source software as such, pure cloud applications, spare parts, and legacy products. A special feature of the CRA is the requirement that the cybersecurity of the product must be confirmed by the manufacturer as part of the CE declaration. In the future, cybersecurity will therefore be on an equal footing with, for example, EMC testing.

The CRA considers products throughout their entire life cycle. Starting with the initial concepts, through actual development and sales, to discontinuation and far beyond.

The key point is to ensure the best possible security at all times. New information about threats comes to light every day. It is therefore essential to keep security up to date with the latest technology and to notify users of new risks.

In addition, appropriate solutions must be offered, for example in the form of firmware updates, configuration adjustments, or changes to access options.

The CRA also includes the obligation to continue providing security updates for a specific period (at least 5 years) after a product has been discontinued. Discontinuation therefore leads to an obligation to continue to enable the usability of the product through security updates.

In the field of industrial automation and communication, IEC 62443, specifically Part 4 (development process and product security), can be used to implement the CRA from today's perspective. In addition, EN 18031 should also be considered for radio-based products.

Machinery Directive

The newly revised Machinery Directive covers machinery and parts of machinery. It is therefore aimed at integrators and machine builders, but also at operators. The focus of the previous Machinery Directive was on protecting people from machinery. Safety was the primary concern.

With the revision of the Machinery Directive as the Machinery Regulation (EU 2023/1230), the concept of protecting the machine from humans, i.e., security, was added.

Important topics such as protecting the machine itself and the machine network from external attackers have been added. The risks posed by digital technologies and deep communication must be mitigated.

ISO 62443, specifically Part 3, can be used to implement the Machinery Directive.

NIS-2 Directive

The NIS-2 Directive focuses on security within the company itself – i.e., not on the products that the company places on the market. The NIS-2 Directive specifically targets companies in the critical infrastructure sector, but – and this is new – also a large number of companies that are suppliers or service providers for critical infrastructure, known as essential or important companies.

The aim of the NIS-2 Directive is to consider the information security of the company as a whole. This is to ensure that neither critical infrastructure can be attacked nor can dangers emanate from service providers or suppliers to critical infrastructure.

ISO 27001 or BSI basic protection are relevant for the implementation of NIS-2. The implementation of this standard enables many companies to meet the requirements. In addition to the implementation of NIS-2, the KRITIS umbrella law and the IT Security Act (2.0) also play an important role for operators of critical infrastructure in Germany.

RED Directive

The RED Directive (EU 2014/53) has been in force since August 2025 and specifically covers products with wireless connectivity (WiFi, Bluetooth, LTE, 5G, etc.). As this class of devices is vulnerable to external attacks via wireless connections, great importance was attached to the security of wireless interfaces at a very early stage. Reconfiguration, firmware updates, and other security-related functions are examined in more detail in the RED Directive.

In the long term, the RED Directive will probably be replaced by the CRA, as the latter already contains corresponding security considerations for wireless solutions. EN 18031 can be used to implement the RED Directive. Since EN 18031 is a new harmonized standard, compliance with the requirements of the standard ensures the conformity of the product with the RED Directive.

There are a number of other regulations, directives, and laws that are relevant or mandatory for specific industries and sectors, such as automotive or medical technology. The above list is sufficient for the time being when considering industrial communication in the factory automation environment.

LEGAL OBLIGATIONS: THE RELEVANT STANDARDS

Standards exist for the technical implementation of the legal requirements, some of which were already created before the aforementioned regulations came into force and were therefore developed in advance.

The need for a unified framework and reliable procedures for industrial security existed even before the current regulations. The standards are currently being adapted in EU committees (e.g., CENELEC) to new requirements such as the CRA and today provide solid guidance for the conformity of products, machines, and companies.

IEC 62443

As the central standard in the field of industrial communication, the international **IEC 62443** series of standards deals with the cybersecurity of industrial automation and control systems (IACS) and takes a holistic approach for operators, integrators, and manufacturers. It therefore affects everyone involved in the manufacture and operation of machines.

It defines the corresponding responsibilities for machine manufacturers, suppliers, and end customers. It defines the respective responsibilities of machine builders, suppliers, and end customers.

The standard is currently divided into **four parts**. **While Part 1 clarifies terminology** and explains general concepts, **Parts 2 to 4 deal** with the **perspectives** of the **product manufacturer**, the **integrator/machine builder**, and the **operator**.

IEC 62443 defines the cybersecurity of industrial automation and control systems (IACS) with a holistic approach for manufacturers, integrators, and operators.

Key concepts of this standard, as well as other standards for IT or radio products, are the **risk-based approach** and the view of security as a **continuous improvement process**.

The risk-based approach forces manufacturers and users to discuss the actual risks posed by an application and to take appropriate measures depending on the level of protection required.

The improvement process requires all participants to exercise discipline in continuously adapting the security of the system or product to new threats and potential attacks.

For a product or machine manufacturer, it starts with the development process. At each stage of the development process, both the safety requirements and the resulting measures must be considered and defined.

In this context, the question arises as to what level of protection the product or system actually requires. Questions regarding how the product or machine is actually used and whether the machine or the goods produced could pose a hazard must be clarified in advance.

In this context, IEC 62443 defines the term "security level." The security level determines who we want to protect ourselves against.

From casual hackers who want to see what they can do to targeted state actors.

IEC 62443 SECURITY LEVELS
Industrial communication networks - Network and system security

General		Policies & Procedures		System		Component / Product	
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	IACS Security Program Ratings	3-2	Security risk assessment and system design	4-2	Technical security requirements for ICAS components
1-3	System security conformance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers				
		2-5	Implementation guidance for IACS asset owners				

Machine builder / Solution provider

Product manufacturer

End customer / Operator / Asset owner

Depending on the product and application, security levels 2 or 3 are relevant in our customers‘ application environments.

As a product manufacturer, it is particularly important to consider the two sub-sections of standard 62443-4-1 and -4-2. Subsection “-4-1” deals with the development process, risk assessment, management of security requirements, and ongoing maintenance of product security. Subsection “-4-2” deals with the individual technical measures that must be considered functionally in terms of product security.

A manufacturer‘s development process can be certified according to subsection “-4-1.” A product can be certified according to subsection “-4-2.” However, without an established and certified development process in accordance with “4-1,” product certification is difficult to achieve.

IEC 62443 is currently being updated and expanded by European standardization committees. The aim is to be able to use it as a harmonized standard for full compliance with the CRA in an industrial environment.

IEC 62443 SECURITY LEVELS

SL 0	No special protection required.
SL 1	Protection against unintentional or accidental injury.
SL 2	Protection against deliberate actions by an attacker with few resources, basic skills and low motivation.
SL 3	Protection against deliberate actions by an attacker with moderate resources, IACS-specific knowledge and moderate motivation.
SL 4	Protection against deliberate actions by an attacker with extensive resources, IACS-specific knowledge and high motivation.

EN 18031

The standard deals with security for products with radio transmission technology in accordance with the RED Directive. The focus here is on the vulnerability of radio technology. Compliance with the requirements of EN 18031 sufficiently fulfills the implementation of the RED Directive.

ISO 27001 / BSI IT Grundschutz

The ISO 27001 series of standards has been an established standard for the implementation and operation of an ISMS (Information Security Management System) in companies for many years. “IT-Grundschutz” is the implementation of the elements of ISO 27001 specified by the BSI for Germany.

An ISMS is designed to ensure that all sensitive information, processes, and IT systems within a company are permanently protected against threats.

The implementation of an ISMS in accordance with ISO 27001 or IT-Grundschutz should enable the essential requirements of the NIS-2 Directive to be met.

SECURITY AT HELMHOLZ: PRACTICE INSTEAD OF THEORY

Helmholz has been addressing the issue of security for a long time. It is not without reason that we have had products such as the “WALL IE” firewall in our range for over 10 years.

What used to be achieved through security-focused planning, design, and penetrationtesting is now and will continue to be achieved through a product development cycle in accordance with IEC 62443-4-1.

Security is not a state of being – it is a process.

Comprehensive employee training, risk-based requirements management for product features and functions, and targeted testing of security requirements ensure the development of secure products.

A central element of both the IEC 62443 standard and the Cyber Resilience Act is the management of new threats and new security risks. What is considered secure today may be compromised tomorrow. Helmholz has a PSIRT team that acts as a continuous monitoring body.

The **Helmholz PSIRT team** consists of trained in-house experts who respond to security reports from suppliers, authorities (e.g., the BSI), customers, or other players in the security environment (vulnerability reporters), compile all information, evaluate it, and implement measures immediately.

We handle external communication (publishing reports and advisories on Helmholz products) in partnership with CERT@VDE.

The goal is to have the development process certified in accordance with IEC 62443-4-1 by TÜV Nord in early 2026.

This is in line with what many other large and small market players do. CERT@VDE is also involved in standardization work and legislative procedures.

Helmholz is a supplier of network products to many industries, including those related to KRITIS. This means that we are classified as an **“important company”** in accordance with the **NIS-2** Directive. The implementation of the resulting requirements of the NIS-2 Directive are therefore relevant for us and will be carried out in 2026.

Our partners in security

Helmholz collaborates with recognized institutions and networks in the field of industrial security to ensure the highest standards in product and information security.

Our partners support us in continuous development, certification, and professional exchange on current security requirements and standards. Together, we ensure that our solutions comply with the latest guidelines and remain trustworthy in the long term.

We would like to thank our partners for their close cooperation and shared commitment to greater security in industry.

Our partners:
Federal Office for Information Security (BSI) | VDE CERT | TeleTrusT | Secuvera

Bundesamt für Sicherheit in der Informationstechnik

VDE CERT

TeleTrusT Pioneers in IT security.

secuvera: Cybersicherheit. Nachhaltig.

CRA READY: HOW HELMHOLZ PREPARES ITS PRODUCTS

The legal requirements and relevant standards mentioned in this document always address components with “digital elements” and a communication interface.

In Helmholz‘s product portfolio, this includes all **products with a communication interface**, such as Ethernet, USB, or wireless. Products with built-in software and communication capabilities are of particular interest here.

Mechanical or electromechanical components such as connectors and cables are not affected by this. Products that are intended for processing digital or analog signals and do not have communication interfaces are also not covered by these regulations. Likewise, unmanaged switches are not considered in depth here.

A special case can be found in products that are already at the end of their product life cycle, such as “NETLink.” If these products are no longer being developed or modified in any way, they can continue to be used as legacy products.

However, the security risks posed by these products must be assessed by the user and secured separately (e.g., with an additional firewall). This is important because legacy products will no longer receive security updates.

From the date the Cyber Resilience Act comes into force, products that have already been discontinued can continue to be sold as spare parts. The security-related assessment of these products is then the responsibility of the user of the products in their machine or system.

As with legacy products, spare parts may require additional security measures in the machine or network design.

All products that fall under the CRA regulation will be gradually adapted by Helmholz in accordance with the requirements of the IEC 62443-4-2 standard. The development process at Helmholz complies with IEC 62443-4-1.

The goal is to be able to provide all products with an extended CE declaration by the time the CRA comes into force in December 2027. Product certification of most Helmholz products by a notified body is not expected to be necessary. However, products that are at the heart of a facility‘s security infrastructure, such as WALL IE, routers, or managed switches, will receive 62443-4-2 certification.

Helmholz GmbH & Co. KG | Hannberger Weg 2 | 91091 Großenseebach | Germany
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.com