Author: Carsten Bokholt
November 2026



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

4 ABOUT US

5 MOTIVATION & VISION

6 RELEVANT REGULATIONS AND GUIDELINES

- Cyber Resilience Act
- Machinery Directive
- NIS-2 Directive

9 LEGAL OBLIGATIONS THE RELEVANT STANDARDS

- IEC 62443
- ISO 27001 / BSI IT baseline protection

13 SECURITY AT HELMHOLZ: PRACTICE INSTEAD OF THEORY

- Security is not a state – it is a process
- Our partners

15 CRA READY: HOW HELMHOLZ PREPARES ITS PRODUCTS

16 CYBER RESILIENCE ACT: THE MOST IMPORTANT QUESTIONS AT A GLANCE

20 EU MACHINERY REGULATION: WHAT MACHINE BUILDERS NEED TO KNOW

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. From the Cyber Resilience Act (CRA) for products with digital elements and the new Machinery Regulation for machine safety to the security of corporate IT and critical infrastructure (NIS-2), there is something for everyone.

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.

The CRA also divides the different product types into security categories. Most products fall into the standard category, such as unmanaged switches, PLCs or operator terminals. In this category, the manufacturer must independently ensure compliance with the CRA using the available standards and issue a CE self-declaration of conformity for each affected product.

In addition, there are Class I and Class II products, such as routers, firewalls and managed switches. For these products, the manufacturer must have the conformity of the products and its development processes assessed by a notified body.

The highest category includes critical products used for the direct operation of critical infrastructure.

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.

To implement the Machinery Regulation, IEC 62443, particularly Part 3, or the upcoming EN 50742 standard, which summarizes the relevant topics of IEC 62443-3, can be used.

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.

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				

Product manufacturer

Machine builder / Solution provider

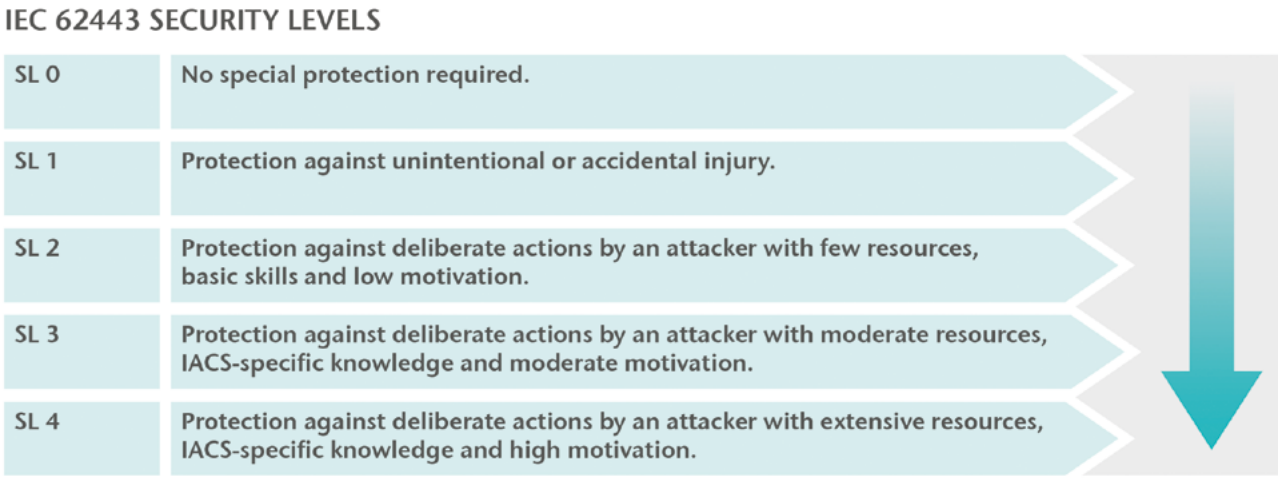
End customer / Operator / Asset owner

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.



ISO 27001 / BSI IT baseline protection

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.

Certification of the development process in accordance with IEC 62443-4-1 by TÜV Nord.

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

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 | die Resilienz GmbH

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.

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. Additional safety measures are necessary in the machine or network design for replacement parts.

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.

CYBER RESILIENCE ACT: THE MOST IMPORTANT QUESTIONS AT A GLANCE

The Cyber Resilience Act introduces new cybersecurity requirements for digital products. The following questions and answers explain the most important regulations and obligations.

What does "CRA-compliant" mean for a product?
A CRA-compliant product meets the essential cybersecurity requirements of the CRA, has undergone a cybersecurity risk assessment, and has processes in place for handling vulnerabilities and security updates.
Following a successful conformity assessment, compliance is documented in the EU Declaration of Conformity, and the product is CE-marked accordingly.
All products that fall within the scope of the CRA and are placed on the EU market (sold!) from December 11, 2027, must comply with the CRA.

Do already installed Helmholz products need to be replaced?
No! In principle, the CRA does not require already installed products to be replaced.
Products sold before December 11, 2027, are generally not retroactively subject to the product requirements of the CRA.
However, a substantial modification to a product after this date may require a reassessment.

Will all Helmholz products be CRA-compliant?
All current Helmholz products affected by the CRA will comply with its requirements.

When will Helmholz products comply with the CRA?
From December 11, 2027, all current Helmholz products will meet the applicable requirements of the Cyber Resilience Act.

Will the products be redesigned to comply with the CRA?
Yes, many products will undergo a redesign.
The products will be modernized and migrated to a modern technical platform. Their form and function will remain unchanged.
The new platform will then enable a longer support period.

What will happen to the old products?
Product variants affected by a redesign will be discontinued shortly thereafter.
However, discontinued products will continue to receive security patches and will still be available as spare parts after the end of 2027.
The CRA explicitly provides for a spare parts exemption.

Are there any products that will no longer be available due to the CRA?
There are some very old products (e.g., MPI adapters or CAN 300 PRO) that will only be available as spare parts from the end of 2027.
A list of these products will be published shortly.

What is the support period for the products?
The support period is determined and documented for each product as part of the CRA conformity assessment.
We are currently aiming for a support period of approximately 8-10 years from the product release date.
The support period will be documented as a fixed date, e.g., "This product will receive security updates until December 31, 2035."
Helmholz may voluntarily extend the originally defined support period for individual products at a later date, for example, when adding new features.

What happens after the security support period ends?
After the published end of the security support period, Helmholz is no longer obligated to provide new security updates.
Helmholz therefore recommends replacing the product in good time with a successor product that is still supported or implementing suitable compensating security measures.

Where is product security documented?
Secure use is documented in the product's "Security Guideline", which can be found in the product manual or as a separate document.
The Security Guideline documents the conditions under which the product can be used securely (intended use), which security capabilities the product provides, and how these should be configured.

What must customers do to ensure secure operation?
The CRA considers product security and secure operation together. Products must be used according to their intended purpose, configured securely, and integrated into a suitable network architecture.
The respective Security Guideline provides information on these requirements.

Where can I find vulnerability reports for the products?
Vulnerability reports concerning Helmholz products are published as advisories via CERT@VDE: (https://certvde.com/en/advisories/vendor/helmholz/)

Where can I find firmware updates?
The latest firmware versions can be found on the Helmholz website under the respective product.
Helmholz does not distinguish between security updates and feature updates.

Is a firmware update available for every vulnerability?
According to the CRA, a vulnerability does not necessarily have to be resolved through a firmware update. Depending on the vulnerability, the risk

may also be addressed through compensating measures outside the product.
Compensating measures may include, for example, changing the configuration or connecting the product to the network differently.
Such a solution will also be documented in an advisory and in the product manual.

Are security updates subject to a fee?
Security updates addressing vulnerabilities are generally provided free of charge.

How can I report vulnerabilities to Helmholz?
Identified or suspected vulnerabilities in Helmholz products can be reported to the PSIRT team at any time (psirt@helmholz.de, https://www.helmholz.de/en/service-support/service/security-psirt/).
Alternatively, vulnerabilities can also be reported via CERT@VDE.

Does Helmholz provide an SBOM with its products?
Helmholz creates and maintains a Software Bill of Materials (SBOM) for relevant products as part of its internal technical documentation and vulnerability monitoring.
The CRA does not require the SBOM to be made publicly available or provided to customers as standard, and Helmholz currently does not plan to do so.
The SBOM will be provided to the responsible authorities (e.g., the BSI) in accordance with legal obligations.

How does Helmholz ensure secure development?
Helmholz develops its products using a secure development process in accordance with IEC/EN 62443-4-1 and the additional requirements of the CRA. The certification of the development process is currently being carried out by TÜV Nord.
Helmholz develops its products entirely in-house (hardware and software) and also manufactures them in its own production facilities. This ensures that product security can be maintained throughout the entire process, from development to manufacturing.

Which standard applies to the products?
All products falling within the scope of the CRA are developed in accordance with IEC/EN 62443-4-2.

What security level do the products have according to IEC 62443-4?
All products falling within the scope of the CRA have at least Security Level 2 (SL-2).

How are “legacy” protocols handled?
Older protocols (e.g., Modbus TCP or RFC 1006) cannot be made “secure” for technical reasons and due to compatibility requirements with existing communication partners.
When using these protocols, the networks must be secured by the machine designer or the customer, for example, through a firewall and strict access restrictions for the affected devices.

How secure is Helmholz as a company?
Helmholz is classified as an “Important Entity” under NIS-2. Corresponding ISO 27001 certification is planned for 2027.

EU MACHINERY REGULATION: WHAT MACHINE BUILDERS NEED TO KNOW

The new EU Machinery Regulation places greater emphasis on the cybersecurity of machines. The following questions and answers provide an overview of the most important requirements.

What does the new Machinery Regulation have to do with cybersecurity?
Manipulation or unintended changes to hardware, software or network communication must not result in the impairment of a machine‘s safety functions.
The Machinery Regulation therefore addresses cybersecurity particularly where a cyberattack could affect functional safety.

What is the difference between the CRA and the Machinery Regulation?
The CRA addresses the cybersecurity of a product with digital elements throughout its lifecycle.
The Machinery Regulation, on the other hand, addresses machine safety.
Cybersecurity becomes relevant when manipulation could compromise the safety of the machine.
Both regulations may therefore apply simultaneously.

If a Helmholz product is CRA-compliant, does that automatically mean the machine complies with the Machinery Regulation?
No. A CRA-compliant communication product can contribute to machine safety, but it does not replace the risk assessment and conformity assessment of the complete machine.

What responsibilities does a machine builder have when using a router, switch or firewall?
As part of the risk assessment, the machine builder must evaluate whether manipulation of the communication system could affect safety functions or other safety-related functions of the machine.
Helmholz‘s secure products support this through comprehensive security features and corresponding documentation.

Does every network component in a machine need special security features?
Not necessarily. The decisive factors are the component‘s function within the machine and the resulting risk.
For example, a simple network component can be secured through network segmentation, firewalls or other organizational and technical measures.

Are PROFINET, Modbus TCP or other unencrypted industrial protocols still permitted under the Machinery Regulation?
In principle, yes. The Machinery Regulation does not prohibit such protocols.
However, the machine manufacturer must consider the risks that may arise from manipulation or un-

authorized access and, where necessary, implement appropriate protective measures.

Will machines be required to have a firewall in the future?
No, the regulation does not prescribe any specific technology.
However, depending on the risk assessment, a firewall, network segmentation or access control may be very suitable protective measures.

What role do Helmholz Security Guidelines play in machinery conformity?
The Security Guideline can provide machine builders with information on secure integration and configuration.
However, responsibility for the machine‘s risk assessment remains with the machine manufacturer.

What does a “substantial modification” of a machine mean?
The new regulation explicitly defines “substantial modification”.
A physical or digital modification not foreseen by the original manufacturer may be considered substantial if it creates a new safety risk or increases an existing risk, thereby requiring new significant protective measures, such as activating a communication protocol.
The person or company carrying out such a modification may consequently become the manufacturer within the meaning of the Machinery Regulation.

Can a firmware or software update also constitute a substantial modification of a machine?
Yes, digital modifications can also be relevant. The decisive factor is whether they affect the safety of the machine.
A standard security update is therefore not automatically considered a substantial modification.
The assessment depends on any additional changes to the firmware and their impact on the machine.

Does a firmware update of a Helmholz device require the entire machine to undergo a new CE conformity assessment?
Normally, not solely because of the update.
However, the machine operator or machine manufacturer must assess whether the firmware changes affect the safety of the machine.
In particular, routine maintenance or repair measures that do not affect compliance with safety requirements are not automatically considered substantial modifications.

Who is responsible if the operator subsequently modifies a machine?
If a company carries out a substantial modification, it may assume the manufacturer‘s obligations for the affected machine and may be required to conduct a new conformity assessment.

What is the significance of remote access under the Machinery Regulation?
Remote access should be designed and operated in such a way that unauthorized access or manipulati-

on cannot compromise safety-related functions.
Authentication, access restrictions and secure configuration are therefore particularly relevant measures for routers and remote maintenance solutions.
Helmholz products provide all the necessary functions for secure remote maintenance operations.

Are machine builders required to install security updates for components?
There is no general obligation to install every update immediately. However, the operator or manufacturer must ensure that the machine continues to operate safely.
A known cybersecurity issue that could affect machine safety must therefore be taken into account in the risk assessment.
Based on this assessment, it can be determined whether machine safety is affected at all and how urgently measures, such as a firmware update, need to be implemented.

What happens if a known vulnerability in a component cannot be resolved?
If this results in a relevant risk to machine safety, technical or organizational measures may be necessary, such as new network segmentation, access restrictions or replacement of the component.

What information does Helmholz provide to machine builders for their risk assessments?
The secure use and configuration of Helmholz products are documented in the respective product‘s Security Guideline.
Security advisories for the products are available via CERT@VDE (https://certvde.com/en/advisories/vendor/helmholz/).
The latest firmware updates can be downloaded free of charge at any time from the respective product page on the Helmholz website.

What role does IEC 62443 play in the Machinery Regulation?
IEC 62443 can serve as a technical framework for industrial cybersecurity, particularly for defense-in-depth, secure components and secure system architectures.
Part 3 of IEC 62443, in particular, provides guidance for machine builders. However, it does not automatically replace the conformity assessment required under the Machinery Regulation.

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

We reserve the right to make changes without notice. Errors and omissions excepted. 11-2026