Autor: Carsten Bokholt
April 2026

WHITEPAPER

INDUSTRIAL SECURITY

VERTRAUEN DURCH SICHERHEIT – SO SCHÜTZT HELMHOLZ DIE INDUSTRIELLE KOMMUNIKATION.

Ein Leitfaden für Hersteller und Betreiber von Maschinen
zum Umgang mit der aktuellen EU-Gesetzgebung.

www.helmholz.de

Helmholz®
COMPATIBLE WITH YOU

INHALTSVERZEICHNIS

ÜBER UNS

Wo Maschinen kommunizieren, schafft Helmholz Vertrauen: mit Technologie, die verbindet, schützt und industrielle Kommunikation einfach sicher macht.

Seit über 35 Jahren entwickelt Helmholz Lösungen, die industrielle Netzwerke effizienter und zukunftsfähiger machen – von der Feldebene bis in die Cloud. Als Spezialist für PROFINET, Industrial Ethernet und IoT setzt Helmholz auf Qualität, Präzision und partnerschaftliches Denken.

Sichere Kommunikation – von der Komponente bis zur Anlage

Unser Ziel: Technik verständlich und Sicherheit selbstverständlich machen. Ob PROFINET, Industrial Ethernet oder IoT – Helmholz bietet die passenden Komponenten für reibungslose Kommunikation in industriellen Anlagen.

Von Switches und Gateways über Firewalls bis hin zu Remote-Access-Lösungen entstehen Systeme, die verbinden, schützen und Prozesse effizienter machen. Alle Produkte werden in Deutschland entwickelt, geprüft und nach DIN ISO 9001:2015 gefertigt – für Qualität, auf die man sich verlassen kann.

Helmholz denkt Automatisierung weiter: mit Security-by-Design, offenen Standards und Lösungen, die den steigenden Anforderungen an Industrial Security gerecht werden.

So unterstützen wir Maschinenbauer, Integratoren und Betreiber dabei, ihre Anlagen zuverlässig, skalierbar und normkonform zu vernetzen.

Helmholz – Compatible with you. Denn echte Partnerschaft ist die Basis sicherer Kommunikation.

MOTIVATION & VISION

Die Sicherheit von Maschinen und Anlagen ist entscheidend für einen stabilen und ausfallsicheren Produktionsprozess. Nur wer seine Kommunikation absichert, sorgt für dauerhaft verfügbare Anlagen.

Spätestens mit neuen Verordnungen wie dem Cyber Resilience Act (CRA) und der Europäischen Maschinenverordnung werden entsprechende Cybersecurity-Maßnahmen nun für jeden Pflicht, der Produkte oder Maschinen in den Verkehr bringt.

Motivation

Bei Helmholz wurde Security schon früh im Unternehmen und in den Produkten mitgedacht. Dieses Dokument soll einen Überblick über die Rechtslage und die relevanten Normen für Hersteller, Maschinenbauer und Endanwender erläutern und den Stand und den Ausblick der Umsetzung bei der Firma Helmholz geben.

Vision

Vertrauen durch Sicherheit! Sicherheit ist mehr als Technik – sie ist Haltung. Helmholz integriert Security by Design in jedes Produkt, um industrielle Kommunikation dauerhaft zu schützen.

Unsere Vision: Vertrauen entsteht dort, wo Sicherheit beginnt.

RELEVANTE VERORDNUNGEN UND RICHTLINIEN

Mit dem Siegeszug der Ethernet-Vernetzung in Fertigungsanlagen gewinnt auch Cybersecurity an zentraler Bedeutung, wie die aktuellen Normen und Richtlinien zeigen.

Der EU-Gesetzgeber hat zu diesem Themenkomplex verschiedene Verordnungen und Richtlinien verfasst oder aktualisiert. EU-Verordnungen sind ohne nationale Gesetzgebung wirksam, wie z.B. der Cyber Resilience Act („CRA“). Dagegen müssen EU-Richtlinien von den EU-Ländern erst in nationale Gesetzgebung umgesetzt werden, wie z.B. „NIS2“.

Cyber Resilience Act

Der Cyber Resilience Act betrachtet Produkte (Komponenten) mit digitalen Elementen. Das kann ein Handy sein, ein elektronisches Spielzeug mit USB, die Waschmaschine mit WLAN, IT-Produkte oder eben auch eine SPS oder ein industrieller Switch. Es geht hierbei um die Verarbeitung, Speicherung, Übertragung von digitalen Daten. Das bezieht sowohl die Hardware als auch die Software inkl. der zum Produkt zugehörige Cloudanwendung mit ein.

Der CRA wird verpflichtend für alle Produkte bei Verkauf ab Dezember 2027. Der CRA kennt aber Ausnahmen. Das sind bereits regulierte Branchen (Automotive, Medical, Aeronautic), Open Source Software als solches, reine Cloudanwendungen, Ersatzteile und Legacy Produkte. Als Besonderheit ist beim CRA die Forderung zu nennen, dass die Cybersicherheit des Produktes im Rahmen der CE-Erklärung vom Hersteller bestätigt werden muss. Die Cybersicherheit steht somit in Zukunft gleichberechtigt z.B. neben einem EMV-Test.

Der CRA betrachtet die Produkte über Ihren gesamten Lebenszyklus. Beginnend bei den ersten Konzepten über die eigentliche Entwicklung, den Verkauf bis hin zur Abkündigung und lange darüber hinaus.

Zentraler Punkt ist die dauerhafte Sicherstellung einer bestmöglichen Fehlerfreiheit in Bezug auf die Security. Täglich werden neue Erkenntnisse zu Bedrohungen bekannt. Daher ist es unabdingbar die Security auf den Stand der Technik zu halten und neue Risiken den Nutzern zu melden.

Zudem sind entsprechende Lösungen anzubieten beispielsweise in Form von Firmwareupdates, eine Anpassung der Konfiguration oder die Veränderung der Zugriffsmöglichkeiten.

Der CRA enthält auch die Verpflichtung – nach einer Produktabkündigung weiterhin für einen spezifischen Zeitraum (mindestens 5 Jahre) – Sicherheitsupdates zur Verfügung stellen zu können. Eine Abkündigung führt also zur Verpflichtung, die Verwendbarkeit des Produktes durch Sicherheitsupdates weiterhin zu ermöglichen.

Im Umfeld der industriellen Automatisierung und Kommunikation kann aus heutiger Sicht die IEC 62443, speziell der Teil 4 (Entwicklungsprozess und Produktsicherheit) heran-gezogen werden, um den CRA umzusetzen. Zusätzlich sollte bei funkbasierten Produkten auch die EN 18031 betrachtet werden.

Maschinenverordnung

Die neu aufgelegte Maschinenverordnung betrachtet Maschinen und Teile von Maschinen. Sie richtet sich somit an den Integrator, bzw. den Maschinenbauer aber auch an den Betreiber. Bisher lag der Fokus der vorangegangenen Maschinenrichtlinie darauf, den Menschen vor der Maschine zu schützen. Safety stand im Vordergrund.

Mit der Neufassung der Maschinenrichtlinie als Maschinenverordnung (EU 2023/1230) wurde die Betrachtungsweise hinzugefügt, die Maschine vor dem Menschen zu schützen, also die Security.

Wichtige Themen wie der Schutz der Maschine selbst und des Maschinennetzwerks vor Angreifern von außen sind hinzugefügt worden. Es gilt die Risiken aus digitalen Technologien und der tiefen Kommunikation abzusichern.

Zur Umsetzung der Maschinenverordnung kann die ISO 62443, speziell der Teil 3, herangezogen werden.

NIS-2 Richtlinie

Die NIS-2 Richtlinie betrachtet die Security im Unternehmen selbst – also nicht um die Produkte, die das Unternehmen in Verkehr bringt. Die NIS-2 Richtlinie hat hierbei speziell Unternehmen im Bereich der Kritischen Infrastruktur im Fokus, aber – und das ist neu – auch eine Vielzahl von Unternehmen, die Zulieferer oder Dienstleister für kritische Infrastruktur sind, die sogenannten wesentlichen oder wichtigen Unternehmen.

Ziel der NIS-2 Richtlinie ist es die Informationssicherheit des Unternehmens als ganzes zu betrachten. Somit soll sichergestellt werden, dass weder eine Kritische Infrastruktur angegriffen werden kann noch Gefahren von den Dienstleistern oder Zulieferern auf die kritische Infrastruktur ausgehen können.

Zur Umsetzung von NIS-2 ist die ISO 27001 oder der BSI-Grundschutz relevant. Mit der Implementierung dieser Norm können die Anforderungen für viele Unternehmen erfüllt werden. Neben der NIS-2 Umsetzung spielt in Deutschland noch das KRITIS-Dachgesetz und das IT-Sicherheitsgesetz (2.0) eine wesentliche Rolle für Betreiber von kritischer Infrastruktur.

RED Richtlinie

Die RED Richtlinie (EU 2014/53) ist seit August 2025 gültig und betrachtet speziell Produkte mit Funkanbindung (WiFi, Bluetooth, LTE, 5G, etc.). Da diese Geräteklasse über Funk von außen angreifbar ist, wurde hier schon sehr früh auf die Sicherheit der Funkschnittstellen wert gelegt. Umkonfiguration, Firmwareupdate und andere sicherheitsrelevanten Funktionen werden in der RED-Richtline genauer betrachtet.

Langfristig wird die RED-Richtlinie wohl vom CRA abgelöst, da dieser bereits entsprechende Sicherheits-Betrachtungen für die Funklösungen enthält. Zur Umsetzung der RED-Richtlinie kann die EN 18031 verwendet werden. Da die EN 18031 eine neue harmonisiert Norm ist, erfüllt die Einhaltung der Vorgaben der Norm die Konformität des Produktes nach der RED-Richtlinie.

Es gibt noch eine Vielzahl weiterer Verordnungen, Richtlinien und Gesetze, die für spezielle Branchen und Sektoren, wie z.B. Automotive oder Medizintechnik, relevant oder verpflichtend sind. Für die Betrachtung der industriellen Kommunikation im Fabrikautomatisierungsumfeld ist o.g. Aufzählung erstmal hinreichend.

GESETZLICHE VERPFLICHTUNGEN: DIE RELEVANTEN NORMEN

Zur technischen Umsetzung der gesetzlichen Vorgaben existieren Normen, von denen einige bereits vor Inkrafttreten der genannten Verordnungen erstellt und daher im Vorfeld entwickelt wurden.

Die Notwendigkeit eines einheitlichen Rahmens und verlässlicher Verfahren für Industrial Security bestand bereits vor den aktuellen Verordnungen. Die Normen werden aktuell in EU-Gremien (z. B. CENELEC) an neue Vorgaben wie den CRA angepasst und bieten heute eine gute Orientierung für die Konformität von Produkten, Maschinen und Unternehmen.

IEC 62443

Als zentrale Norm im Bereich der industriellen Kommunikation befasst sich die internationale Normenreihe **IEC 62443** mit der Cybersicherheit von „Industrial Automation and Control Systems“ (IACS) und verfolgt dabei einen ganzheitlichen Ansatz für Betreiber, Integratoren und Hersteller.

Sie betrifft also alle, die an der Herstellung und dem Betrieb von Maschinen beteiligt sind. Entsprechende Verantwortlichkeiten für Maschinenbauer, Zulieferer und Endkunden werden dort definiert.

Aktuell teilt sich die **Norm in 4 Teile** auf. Während **Teil 1 Begrifflichkeiten** klärt und **generelle Konzepte** erläutert, betreffen die **Teile 2 bis 4** aus **Sicht** des **Produktherstellers**, des **Integrators/ Maschinenbauers** sowie des **Betreibers**.

Die IEC 62443 definiert die Cybersicherheit industrieller Automatisierungs- und Steuerungssysteme (IACS) mit einem ganzheitlichen Ansatz für Hersteller, Integratoren und Betreiber.

Wesentliche Bestandteile dieser Norm sowie anderer Normen für die IT oder Funkprodukte, sind der **risikobasierte Ansatz** und die Betrachtung der Security als immerwährender **Verbesserungsprozess**.

Der risikobasierte Ansatz zwingt einen Hersteller oder Anwender immer dazu, die tatsächliche Gefährdung einer Anwendung zu diskutieren und je nach Schutzbedarf angemessene Maßnahmen zu ergreifen.

Der Verbesserungsprozess fordert von allen Teilnehmern eine Disziplin, die Sicherheit der Anlage oder des Produkts fortwährend an neue Bedrohungen und Angriffsmöglichkeiten anzupassen.

Für einen Produkt- oder Maschinenhersteller fängt es mit dem Entwicklungsprozess an. In jeder Phase des Entwicklungsprozesses sind sowohl die Sicherheitsanforderungen als auch die daraus folgenden Maßnahmen zu betrachten und festzulegen.

In diesem Zusammenhang stellt sich die Frage, welchen Schutzbedarf das Produkt oder die Anlage überhaupt hat. Fragestellungen auf welche Art das Produkt oder die Maschine überhaupt eingesetzt wird und ob von der Maschine oder dem produzierten Gut eine Gefahr ausgehen kann, sind vorab zu klären.

In diesem Zusammenhang definiert die IEC 62443 den Begriff des Security Levels. Der Security Level legt fest, gegen wen wir uns absichern wollen.

Vom Gelegenheitshacker, der mal probieren will was möglich ist, bis zum gezielt eingesetzten staatlichen Akteur.

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				

End customer / Operator / Asset owner

Machine builder / Solution provider

Product manufacturer

Im Anwendungsumfeld unserer Kunden sind je nach Produkt und Einsatzfall die Security Level 2 oder 3 relevant.

Speziell als Produkthersteller sind die zwei Teilbereiche der Norm 62443-4-1 und -4-2 zu betrachten. Im Teilbereich „-4-1“ geht es um den Entwicklungsprozess, die Risikobeurteilung, das Management der Sicherheitsanforderungen und die fortwährende Aufrechterhaltung der Sicherheit des Produkts. Im Teilbereich „-4-2“ geht es um die einzelnen technischen Maßnahmen, die zur Produktsicherheit funktional zu betrachten sind.

Den Entwicklungsprozess eines Herstellers kann man nach dem Teilbereich „-4-1“ zertifizieren lassen. Ein Produkt kann nach dem Teilbereich „-4-2“ zertifiziert werden. Ohne einen etablierten und zertifizierten Entwicklungsprozess gemäß „4-1“ ist eine Produktzertifizierung aber nur schwer machbar.

Derzeit wird die IEC 62443 in den europäischen Normungsgremien aktualisiert und erweitert. Ziel ist es, diese als harmonisierte Norm zur Erfüllung des CRA im industriellen Umfeld vollständig nutzten zu können.

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

Die Norm behandelt die Security für Produkte mit Funkübertragungstechnik gemäß der RED-Richtlinie. Es wird hierbei ein der Fokus auf die Angreifbarkeit der Funktechnik gelegt. Die Einhaltung der Forderungen aus der EN 18031 erfüllt die Umsetzung der RED-Richtlinie hinreichend.

ISO 27001 / BSI IT-Grundschutz

Die ISO 27001 Normenreihe ist bereits seit vielen Jahren eine etablierte Norm zur Implementierung und Betrieb eines ISMS (Informations-Sicherheits Management System) im Unternehmen. Der „IT-Grundschutz“ ist die vom BSI für Deutschland konkretisierte Umsetzung der Elemente des ISO 27001.

Ein ISMS soll sicherstellen, dass alle schützenswerten Informationen, Prozesse und IT-Systeme des Unternehmens dauerhaft vor Bedrohungen geschützt sind.

Mit der Implementierung eines ISMS gemäß ISO 27001 oder IT-Grundschutz sollten die wesentlichen Forderungen der NIS-2 Richtlinie erfüllt werden können.

SECURITY BEI HELMHOLZ: PRAXIS STATT THEORIE

Helmholz beschäftigt sich schon lange mit dem Thema Security. Nicht umsonst haben wir bereits seit über 10 Jahren Produkte wie die Firewall „WALL IE“ im Programm.

Was früher durch eine sicherheitsgerichtete Planung, Konzeption und PEN-Testing erreicht wurde, wird heute und in Zukunft durch einen Produktentwicklungszyklus gemäß IEC 62443-4-1 betrieben.

Security ist kein Zustand – sondern ein Prozess.

Umfassende Schulungen der Mitarbeiter, ein risikobasiertes Anforderungsmanagement für Produkt-Features und Funktionen sowie das gezielte Testen der Sicherheitsanforderungen gewährleisten die Entwicklung von sicheren Produkten.

Ein zentrales Element der IEC 62443 Norm als auch im Cyber Resilience Act, ist das Management von neuen Bedrohungen und neuen Sicherheitsrisiken. Was heute noch als sicher gilt, kann morgen schon kompromittiert sein. Als kontinuierliches Wachorgan gibt es bei Helmholz dafür das PSIRT-Team.

Das **Helmholz PSIRT-Team** besteht aus geschulten Experten im Haus, welche auf Sicherheitsmeldungen von Lieferanten, Behörden (z.B. dem BSI), Kunden oder anderen Akteuren im Sicherheitsumfeld (Schwachstellen-Melder) reagieren und alle Informationen zusammentragen, diese bewerten und Maßnahmen unverzüglich umsetzen.

Ziel ist die Zertifizierung des Entwicklungsprozesses gemäß IEC 62443-4-1 durch den TÜV Nord bis Herbst 2026.

Die Kommunikation nach außen (das Veröffentlichen von Meldungen und Advisories zu den Helmholz Produkten), betreiben wir in einer Partnerschaft mit dem CERT@VDE.

Im Gleichklang wie es auch viele andere große und kleine Marktbegleiter machen. Das CERT@VDE ist auch an der Normungsarbeit und den Verfahren zur Gesetzgebung beteiligt.

Helmholz ist Zulieferer von Netzwerkprodukten in viele Branchen, u.a. auch in den KRITIS nahen Bereich. Dadurch sind wir gemäß der **NIS-2** Richtlinie als **„wichtiges Unternehmen“** einzustufen. Die Umsetzung der hieraus resultierenden Anforderungen der NIS-2 Richtlinie sind für uns somit relevant und werden 2026 durchgeführt.

Unsere Partner zum Thema Sicherheit

Helmholz arbeitet im Bereich Industrial Security mit anerkannten Institutionen und Netzwerken zusammen, um höchste Standards in Produkt- und Informationssicherheit zu gewährleisten.

Unsere Partner unterstützen uns bei der kontinuierlichen Weiterentwicklung, Zertifizierung und im fachlichen Austausch zu aktuellen Sicherheitsanforderungen und Normen. Gemeinsam stellen wir sicher, dass unsere Lösungen den neuesten Richtlinien entsprechen und langfristig vertrauenswürdig bleiben.

Wir danken unseren Partnern für die enge Zusammenarbeit und das gemeinsame Engagement für mehr Sicherheit in der Industrie.

Unsere Partner:
Bundesamt für Sicherheit in der Informationstechnik (BSI) | VDE CERT | TeleTrusT | Secuvera

Bundesamt für Sicherheit in der Informationstechnik

VDE CERT

TeleTrusT Pioneers in IT security.

secuvera: Cybersicherheit. Nachhaltig.

CRA READY: SO BEREITET HELMHOLZ SEINE PRODUKTE VOR

Die in diesem Dokument genannten gesetzlichen Vorgaben und die hierbei relevanten Normen adressieren immer Komponenten mit „digitalen Elementen“ und einer Kommunikationsschnittstelle.

Im Produktportfolio der Firma Helmholz sind dies alle **Produkte mit einer Kommunikationsschnittstelle**, wie Ethernet, USB oder auch Funk. Insbesondere Produkte mit eingebauter Software und einer Kommunikationsmöglichkeit sind hier vorrangig zu betrachten.

Mechanische- oder elektromechanische Komponenten wie bspw. Stecker und Kabel, sind hiervon nicht betroffen. Auch Produkte, die zur Verarbeitung von digitalen oder analogen Signalen gedacht sind und keine Kommunikationsschnittstellen haben, fallen nicht unter diese Regulierungen. Ebenso sind unmanaged Switche hier nicht in der Tiefe zu betrachten.

Ab dem Zeitpunkt des Inkrafttretens des Cyber Resilience Act können Produkte, die bereits abgekündigt sind, auch weiterhin als **Ersatzteile** verkauft werden. Die sicherheitsrelvante Betrachtung dieser Produkte obliegt dann dem Anwender der Produkte in seiner Maschine oder Anlage. Bei Ersatzteilen sind zusätzliche Sicherheitsmaßnahmen im Maschinen- oder Netzwerkdesign notwendig.

Alle Produkte, die unter die Regulierung des CRA fallen, werden von Helmholz nach und nach gemäß den Vorgaben der Norm IEC 62443-4-2 angepasst. Der Entwicklungsprozess bei Helmholz arbeitet dabei gemäß IEC 62443-4-1.

Ziel ist es bis zum Inkrafttreten des CRAs im Dezember 2027 alle Produkte mit einer erweiterten CE-Erklärung ausstatten zu können. Eine Produktzertifizierung der meisten Helmholz Produkte bei einer notifizierten Stelle ist voraussichtlich nicht notwendig. Produkte, die im Zentrum der Security-Infrastruktur einer Anlage stehen, wie z.B. WALL IE, den Routern oder den managed Switchen, werden aber eine 62443-4-2 Zertifizierung erhalten.

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.de