



wieland



MASCHINEN SICHER IN DIE
ZUKUNFT BRINGEN

**CYBER
RESILIENCE ACT
EINFACH
UMGESETZT**

Wieland Electric | Franca Hopf

WIELAND ELECTRIC

1910
GRÜNDUNG



2
PRODUKTIONSSTÄTTEN

UNGEFÄHR
25,000
PRODUKTE IM
SORTIMENT

ÜBER
70
VERTRIEBSPARTNER
WELTWEIT

14
TOCHTERGESELLSCHAFTEN

FUNKTIONALE SICHERHEIT IST UNSER KERNGESCHÄFT

SICHERHEITSTECHNIK

- Lösungen vom Sicherheitsrelais bis zur Sensorik
- Entwickelt und gefertigt in Deutschland

SERVICE

- Von der Risikobeurteilung bis zur Validierung
- Performance Level, Dokumentation und CE

NORMUNG & WISSEN

- Mitarbeit im Normungsgremien
- Seminare und Workshops zu funktionaler Sicherheit, MVO und CRA



Sicherheitsrelais



Programmierbare Sicherheitssteuerung



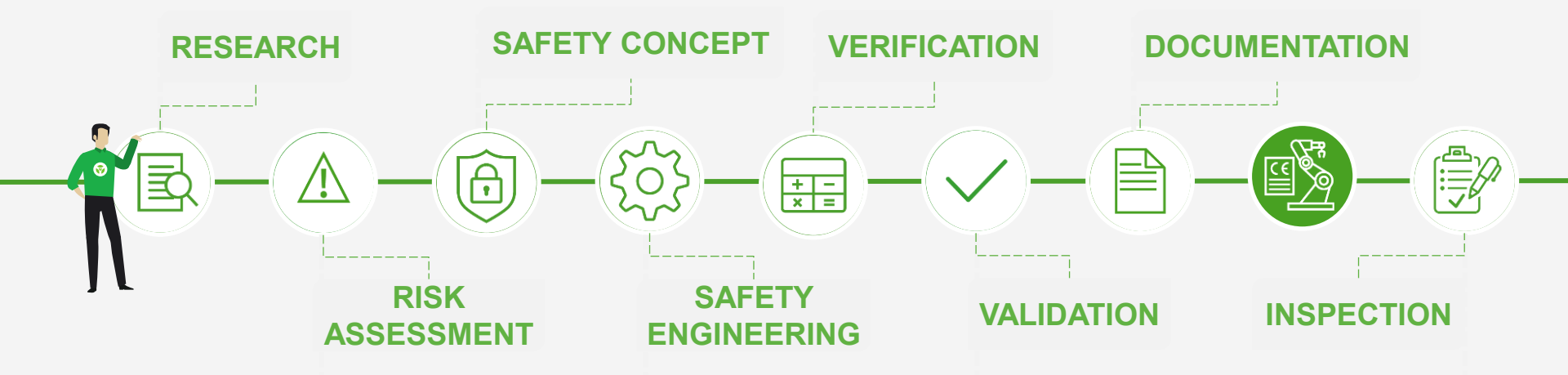
Sicherheitsschalter



Sicherheitslichtgitter

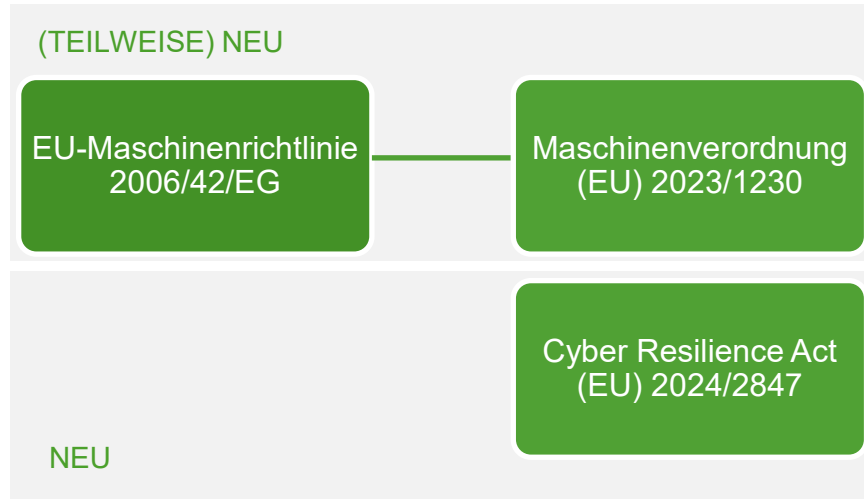
EN ISO 12100 · EN ISO 13849 · IEC 62061 · IEC 62443 – Safety-Erfahrung als Basis für Security

WIELAND ELECTRIC – SAFETY SERVICE & TRAINING



NEUE ANFORDERUNGEN AN MASCHINEN

Maschinen entwickeln sich von isolierten Systemen zu vernetzten, softwarebasierten Systemen.



Regulatorisch entstehen zwei Perspektiven:

- Maschinenverordnung:
Schutz der Menschen vor der Maschine
- Cyber Resilience Act:
Schutz der Maschinen vor dem Menschen



Herausforderung für Maschinenbauer:

- Zwei Regulierungen
- Unterschiedliche Denkweisen
- Aber: gleiche Systeme

CHARAKTER DES CRA INKL. FRISTEN

11.09.2026

Schwachstellenmeldeweg
im Rahmen des
Schwachstellenmanagements

Produkte mit digitalen Elementen

Horizontaler EU-Rechtsakt für Hardware- und Softwareprodukte, die direkt oder indirekt mit anderen Geräten oder Netzwerken verbunden werden können.

11.12.2027

Vollumfängliche
Anwendung

Cyberisiken über den gesamten Produktlebenszyklus

Hersteller müssen Cyberisiken von der Entwicklung bis zum Ende des Supportzeitraums betrachten.

Cybersecurity ist eine verbindliche Produkteigenschaft für die CE-Konformität und Voraussetzung für den EU-Marktzugang.

Schnittstellen

z.B. USB | Ethernet | WLAN | Feldbus | HMI | Engineering | Fernwartung | Cloud

Jede Schnittstelle kann einen Zugangsweg zum Produkt darstellen und muss in der Cybersecurity-Risikobeurteilung berücksichtigt werden.

FEHLENDE EINHALTUNG GEFÄHRDET DIE CE-KENNZEICHNUNG



Neue Vorschriften zur CE-Konformität

CE steht nicht mehr nur für funktionale Sicherheit

CE ist bereits anspruchsvoll, jetzt wird Security Teil davon

Maschinenverordnung (MVO)

- Mechanische Sicherheit
- Funktionale Sicherheit
- Sichere Maschinenkonstruktion

NEU Software- und digitale Sicherheitsaspekte

Cyber Resilience Act (CRA)

- Cybersicherheit vernetzter Produkte/Systeme
- Risikobewertung der Cybersicherheit
- Secure-by-Design-Anforderungen
- Schwachstellenmanagement
- Sicherheitsupdates über den Lebenszyklus

NEU

ZENTRALE ANFORDERUNGEN

Produktbezogene Cybersecurity-Risikoanalyse

Digitale Risiken identifizieren, bewerten und reduzieren über den kompletten Lebenszyklus.



Security by Design

Cybersecurity muss von Beginn an in die Produkteigenschaften einfließen.



Security by Default

Default-Konfiguration muss bei Auslieferung sicher sein und darf zu keiner gefährlichen Situation führen.



Schwachstellenmanagement & Updates

Prozess für Meldewege und Beseitigung von Schwachstellen
Update-Prozesse über Lebenszyklus



Dokumentation

Transparenz über eingesetzte Software (SBOM)
Security Information (Annahmen zum sicheren Betrieb)

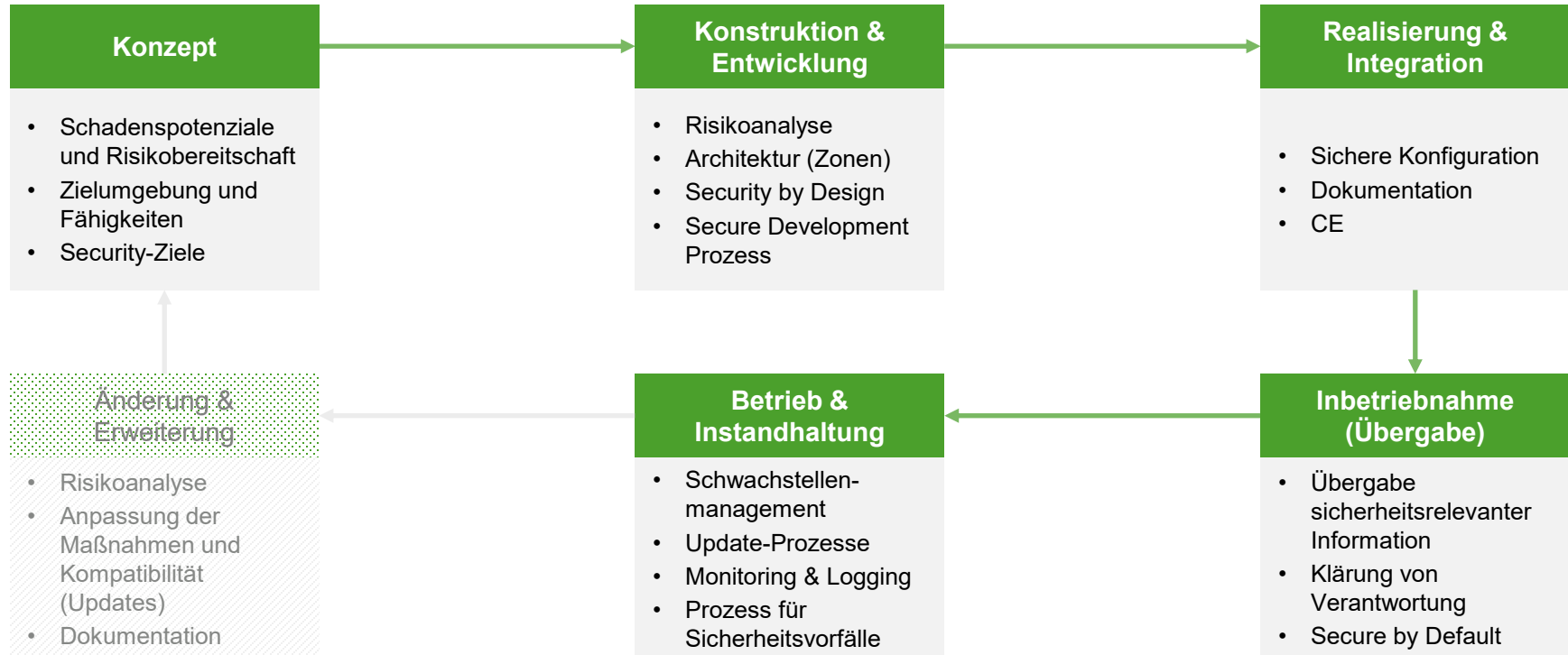


Konformitätsbewertung

Cybersecurity als Teil der CE-Konformität.



IT-MAßNAHMEN IM MASCHINEN-LEBENSZYKLUS



CYBERSECURITY: FEHLANNAHMEN & EINORDNUNG



„Cybersecurity ist ein IT-Thema.“



„Cybersecurity betrifft nur den Betrieb beim Kunden.“



„Cybersecurity kann man später dranbauen.“



„Wenn die Maschine sicher (Safety) ist, passt Cybersecurity automatisch.“



„Wir müssen IEC 62443 zertifiziert sein.“



„Wenn die eingesetzten Produkte secure und zertifiziert sind, erfüllen wir den CRA.“



„Wir müssen ein Security Level bestimmen.“ oder „Wir brauchen Security Level 4.“



„Für alles, was beim Kunden passiert, haftet der Hersteller.“



„Jeder Kunde muss aktiv über eine Schwachstelle informiert werden (Security Advisories).“

VERANTWORTUNG FÜR CYBERRISIKEN

Risikobasierter Ansatz

- Der CRA fordert eine systematische Identifikation und Bewertung
- Nicht jede Schwachstelle muss beseitigt werden

Verantwortung der Unternehmen

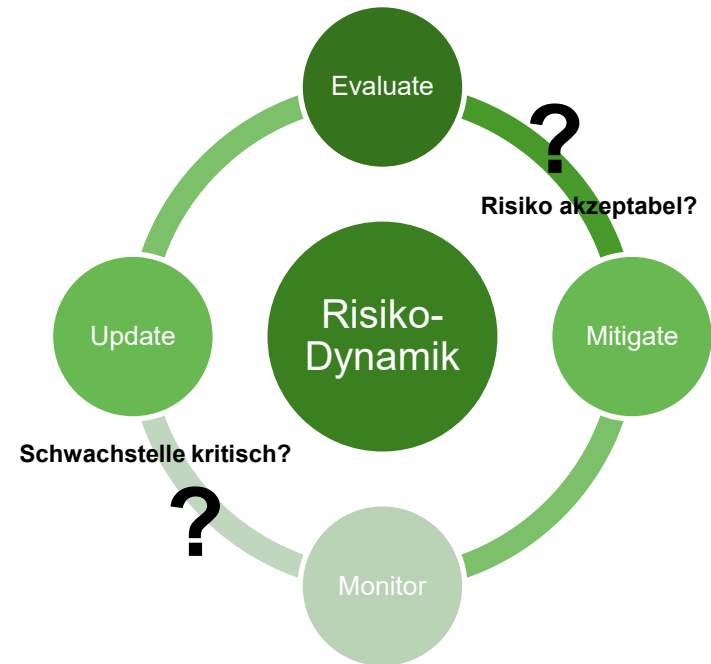
- Unternehmen sind konkret verantwortlich für Cybersecurity-Risiken ihrer Produkte
- Bewusste Verantwortungsübernahme



Akzeptables Risiko

Abhängig von:

- Geschäftsmodell
- Markt
- Einsatzkontext
- potenziellen Auswirkungen.



ANALYSE STATT ENTSCHEIDUNG

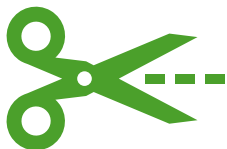


IT- und Security-Teams

Identifikation von Bedrohungen

Analyse von Schwachstellen

Vorschlag technischer Lösungen



Verantwortlichkeiten trennen

Trennung von technischer Analyse und geschäftlichen Risikoentscheidungen

Definition von Verantwortungen



Entscheidungen auf Managementebene

Finale Entscheidungen über akzeptables Risiko durch Management

Basis: technische Grundlagen

WIELAND ALS PARTNER

- 1 Einordnen**
Welche Rolle spiele ich in den neuen Regularien?
- 2 Perspektive einnehmen**
Was ist insbesondere für meine Maschine/ für mein System gültig?
- 3 Erklären**
Was bedeuten die Anforderungen für die Umsetzung in der Praxis?
- 4 Status definieren**
Inwiefern sind meine Prozesse und Unterlagen bereits geeignet?

Mitarbeit in Normungsgremien

"Machinery Expert Group" European Commission (Scholle)

DKE/AK 931.1.2 Cyber security for IACS
(IEC 62443)

NA 095-01-01 GA (ISO 12100)

NA 095-01-03 GA – Controls
(ISO 13849 series)

NA 060-48-02 AA – Emergency stop
(ISO 13850/13851/14118)

NFPA

Mechanical Safety Design Subcommittee of National Technical
Committee 208 of Safety of Machinery of Standardization
Administration of China

SEMINAR: CYBERSECURITY IM MASCHINENBAU



ANGEBOT

EXPERTISE DIREKT AUS DEM NORMUNGSGREMIUM

"Machinery Expert Group" European Commission
DKE/AK 931.1.2 Cyber security for IACS
(IEC 62443)

DIE THEMEN IM ÜBERBLICK

- 01 Warum Cybersecurity zum Pflichtthema wird
- 02 Was MVO und CRA konkret verlangen
- 03 Der Maschinen-Lebenszyklus als Leitlinie
- 04 Cyber-Risikobeurteilung statt klassischer Risikoanalyse
- 05 Security by Design: Zonen, sichere Defaults, Updates
- 06 Übergabe, Dokumentation und Verantwortlichkeiten
- 07 Take-aways und nächste Schritte für alle Rollen

AUF EINEN BLICK

- Praxisnah statt IT-Detailtiefe
- Für Hersteller- und Betreiberrollen
- Bezug zu IEC 62443 und CRA-Pflichten
- Inhouse oder online, mit Checkliste und Umsetzungsfahrplan

Sprechen Sie uns gerne an.

VIELEN DANK.



Kommen Sie vorbei! Stand: **431**



www.wieland-electric.com



training@wieland-electric.com