SAFETY meets SECURITY

So gelingt der ganzheitliche Schutz nach MVO, NIS2 & CRA

Thorsten Knöner

PHOENIX CONTACT Deutschland GmbH
Produktmanager SPS und I/O-Systeme


Wir alle sind gesetzlich dazu verpflichtet, uns
vor Cyber-Attacken zu schützen.

Safety meets Security

Neue gesetzliche Anforderungen für die Industrie

NIS 2

CRA

MVO

Safety meets Security

Neue gesetzliche Anforderungen | NIS2

- NIS= Network & Information Security
- Richtlinie der EU, die Mindestanforderungen an die Cybersicherheit für wesentliche und wichtige Einrichtungen festlegt
- Die Einhaltung dieser Anforderungen muss von der Geschäftsleitung des Unternehmens im Einklang mit den nationalen Rechtsvorschriften überwacht werden und macht diese haftbar
- Überführung in nationales Recht in 2025 erwartet

Safety meets Security

Neue gesetzliche Anforderungen | NIS2

Wesentliche Einrichtungen

Alle Unternehmen >250 Beschäftigten in den Annex I – Sektoren

Wichtige Einrichtungen

Alle Unternehmen >50 Beschäftigten in den Annex I – Sektoren
und alle Unternehmen >250 Beschäftigten in den Annex II – Sektoren

Kleinst- und Kleinunternehmen

Generell ausgeschlossen

Unternehmen mit einem Umsatz von <10 Mio. € oder <50 Beschäftigten

Ausnahmen werden definiert

Annex I Sektoren

- Energie
- Transport
- Bankwesen
- Finanzmarkt-infrastrukturen
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- IT-Service Management
- Öffentliche Verwaltung
- Luftfahrt
- + alle kritischen Einrichtungen im Sinne der Richtlinie (COM(2020) 829)

Annex II Sektoren

- Post- und Kurierdienste
- Abfallwirtschaft
- Herstellung, Produktion und Vertrieb von Chemikalien
- Lebensmittelproduktion, -verarbeitung und -vertrieb
- produzierendes Gewerbe
- Digitale Dienstleister
- Forschung

Safety meets Security

Neue gesetzliche Anforderungen

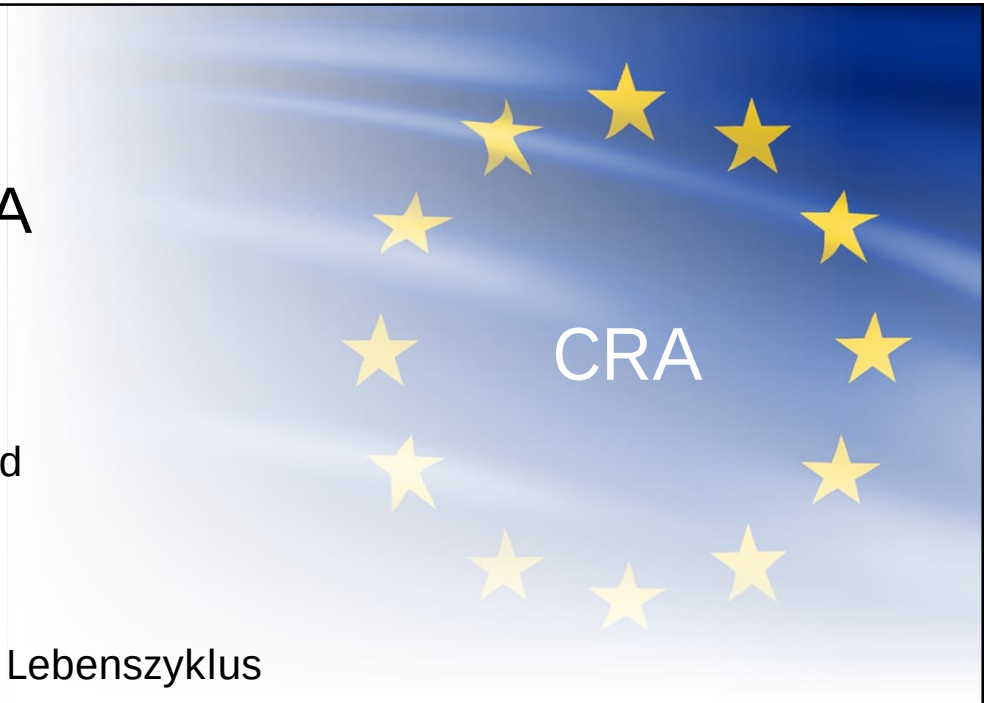
NIS 2

CRA

MVO

Safety meets Security

Neue gesetzliche Anforderungen | CRA



- CRA= Cyber Resilience Act

  (CRV = Cyber-Resilienzverordnung)
- Neue EU-Cybersicherheitsverordnung für digitale Hard- und Softwareprodukte
- Verbindliche Cyber-Security-Anforderungen für Hardware- und Softwareprodukte über ihren gesamten Lebenszyklus
- 11. September 2026 Meldepflicht aller Schwachstellen
- 11. Dezember 2027 Anforderungen müssen eingehalten werden

Safety meets Security

Neue gesetzliche Anforderungen | CRA

Wichtige Produkte II	Wichtige Produkte I	Gängige Produkte
Bewertung durch Dritte	Anwendung einer Norm oder Bewertung durch Dritte	Selbstbewertung
Kriterien: Funktionalität (z. B. kritische Software), Verwendungszweck (z. B. industrielle Steuerung/ NIS2), weitere Kriterien (z. B. Ausmaß der Auswirkungen)		Kriterien: n/a
Beispiele: ▪ Betriebssysteme ▪ Industrielle Firewalls ▪ CPUs ▪ Secure – Elemente ▪ etc	Beispiele: ▪ Passwort-Manager ▪ Netzwerkschnittstellen ▪ Firewalls ▪ Mikrocontroller ▪ etc	Beispiele: ▪ Fotobearbeitungssoftware ▪ Textverarbeitung ▪ Intelligente Lautsprecher ▪ Festplatten ▪ Spiele ▪ etc

Safety meets Security

Neue gesetzliche Anforderungen | CRA

Pflichten des Herstellers:

Cybersicherheit wird in der Planungs-, Design-, Entwicklungs-, Produktions-, Liefer- und Wartungsphase berücksichtigt

Alle Cybersicherheitsrisiken sind dokumentiert

Die Hersteller müssen aktiv ausgenutzte Schwachstellen und Vorfälle melden

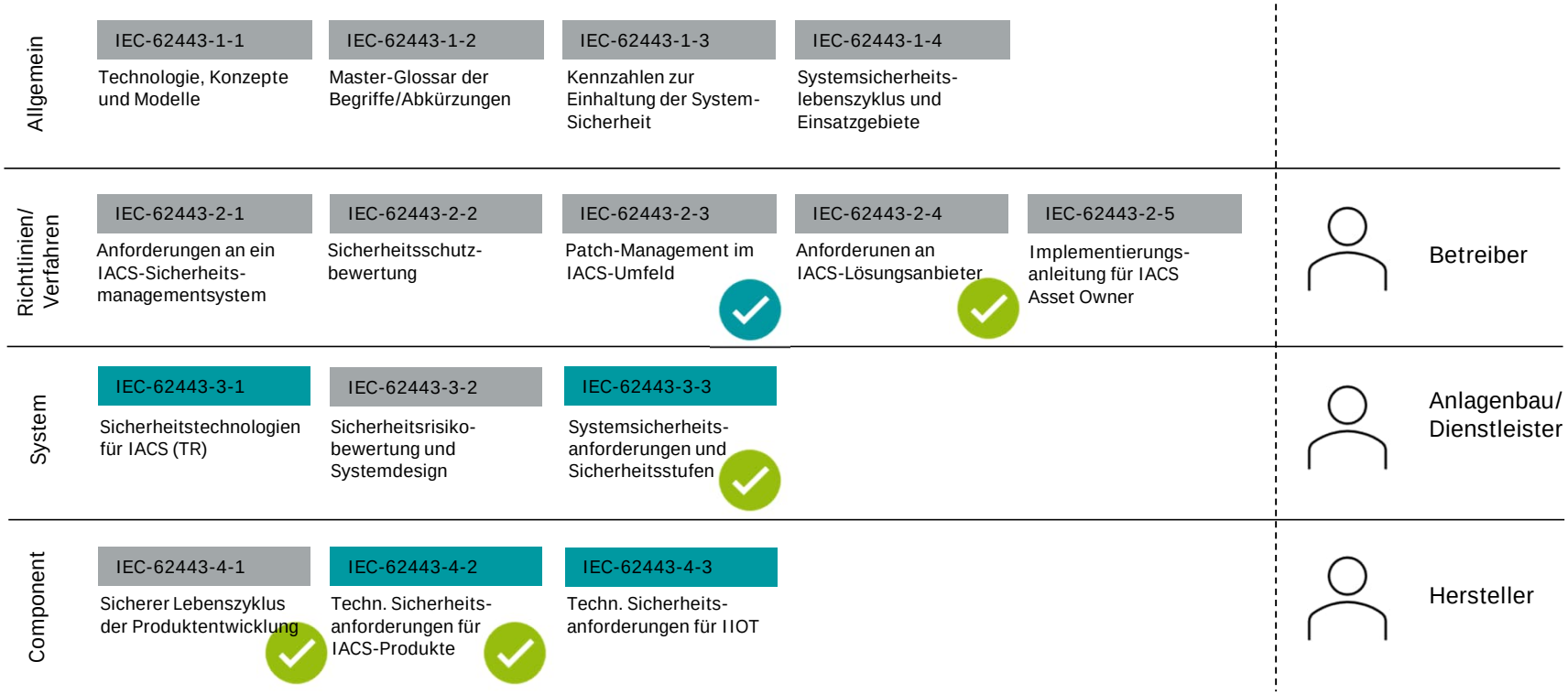
Für die erwartete Produktlebensdauer oder für einen Zeitraum von fünf Jahren (je nachdem, welcher Zeitraum kürzer ist) werden Schwachstellen effektiv behandelt

Klare und verständliche Anweisungen für die Verwendung von Produkten mit digitalen Elementen

Sicherheitsupdates, die mindestens fünf Jahre lang verfügbar sein müssen

Safety meets Security

Die internationale Normenreihe IEC 62443



Safety meets Security

Neue gesetzliche Anforderungen

NIS 2

CRA

MVO

Safety meets Security

Neue gesetzliche Anforderungen | MVO

- MVO = Maschinenverordnung
- Aus der Maschinenrichtlinie 2006/42/EG wird die Maschinenverordnung (EU) 2023/1230
- Grundlegende Gesundheits- und Schutzanforderungen an Maschinen
- Grundlage für Konformitätserklärung & CE-Kennzeichnung einer Maschine
- Gesetzlich verpflichtend für Hersteller & Inverkehrbringer von Maschinen
- Verbindliche Umsetzung ab 20. Januar 2027

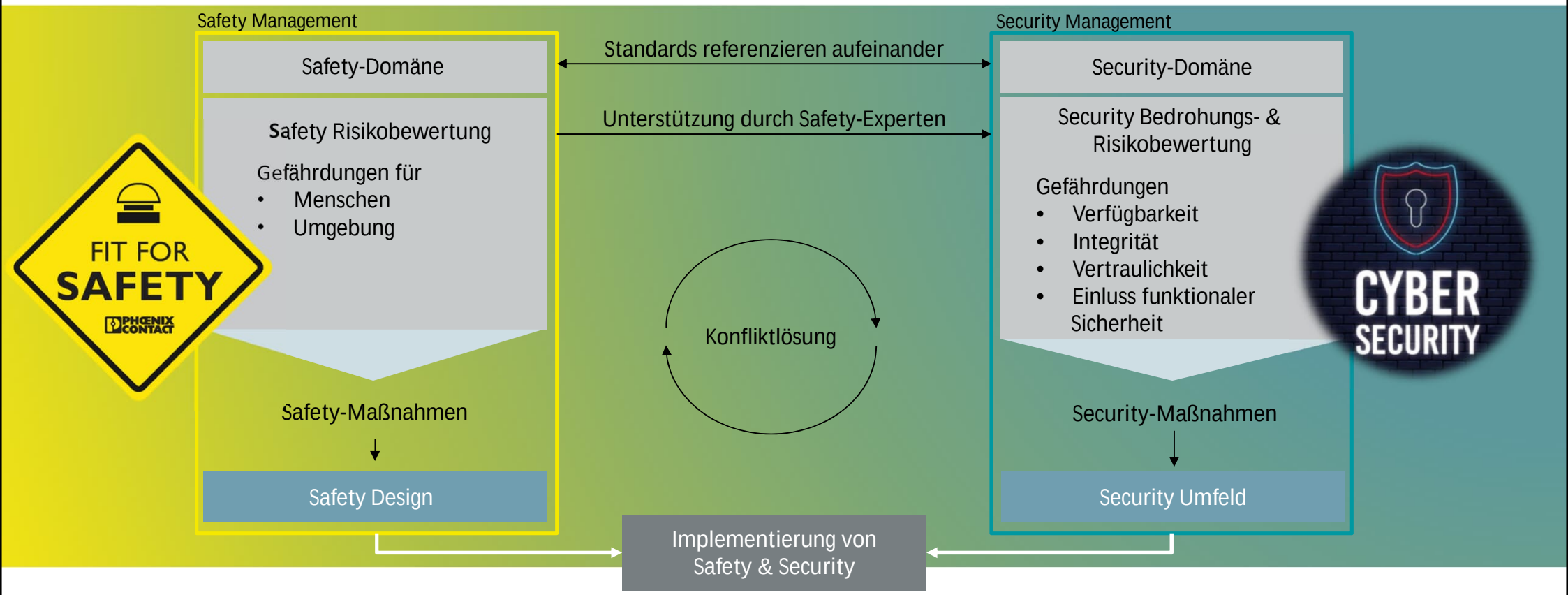
Safety meets Security

Neue gesetzliche Anforderungen | MVO

- Sichere Software gilt fortan als Sicherheitskomponente
- Betriebsanleitungen und Konformitätserklärungen dürfen digital bereitgestellt werden
- Wesentliche Veränderungen einer Maschine werden von der MVO betrachtet
- Anhang III Abs. 1.1.9 Schutz gegen Korrumpierung
  - Externe Zugriffe auf das Maschinenprodukt dürfen nicht zu gefährlichen Situationen führen
  - Hardwarekomponenten müssen so konstruiert sein, dass beabsichtigte und unbeabsichtigte Eingriffe/Änderungen des Systems nicht möglich sind
  - Zugriffs- & Änderungsprotokollierung

Safety meets Security

Zwei Welten treffen sich



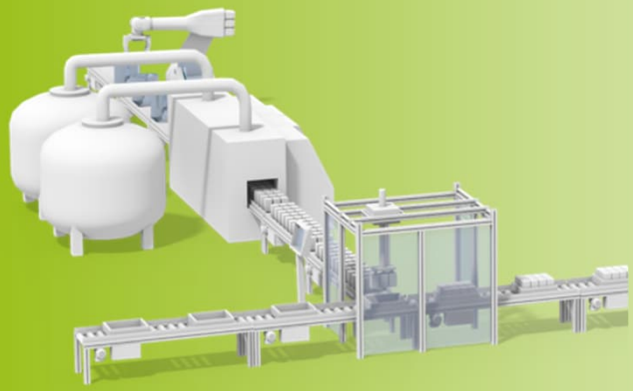
Resultierende Herausforderungen

Maschinen- und Anlagenhersteller

- MVO
  - Schutz gegen Korrumpierung
  - Grundlegende Schutzanforderungen
- NIS 2
  - Lieferkettenmanagement (Betroffene Betreiber werden als Kunde den Hersteller vertraglich verpflichten)
- CRA
  - Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (auch Maschinen)

Resultierende Herausforderungen

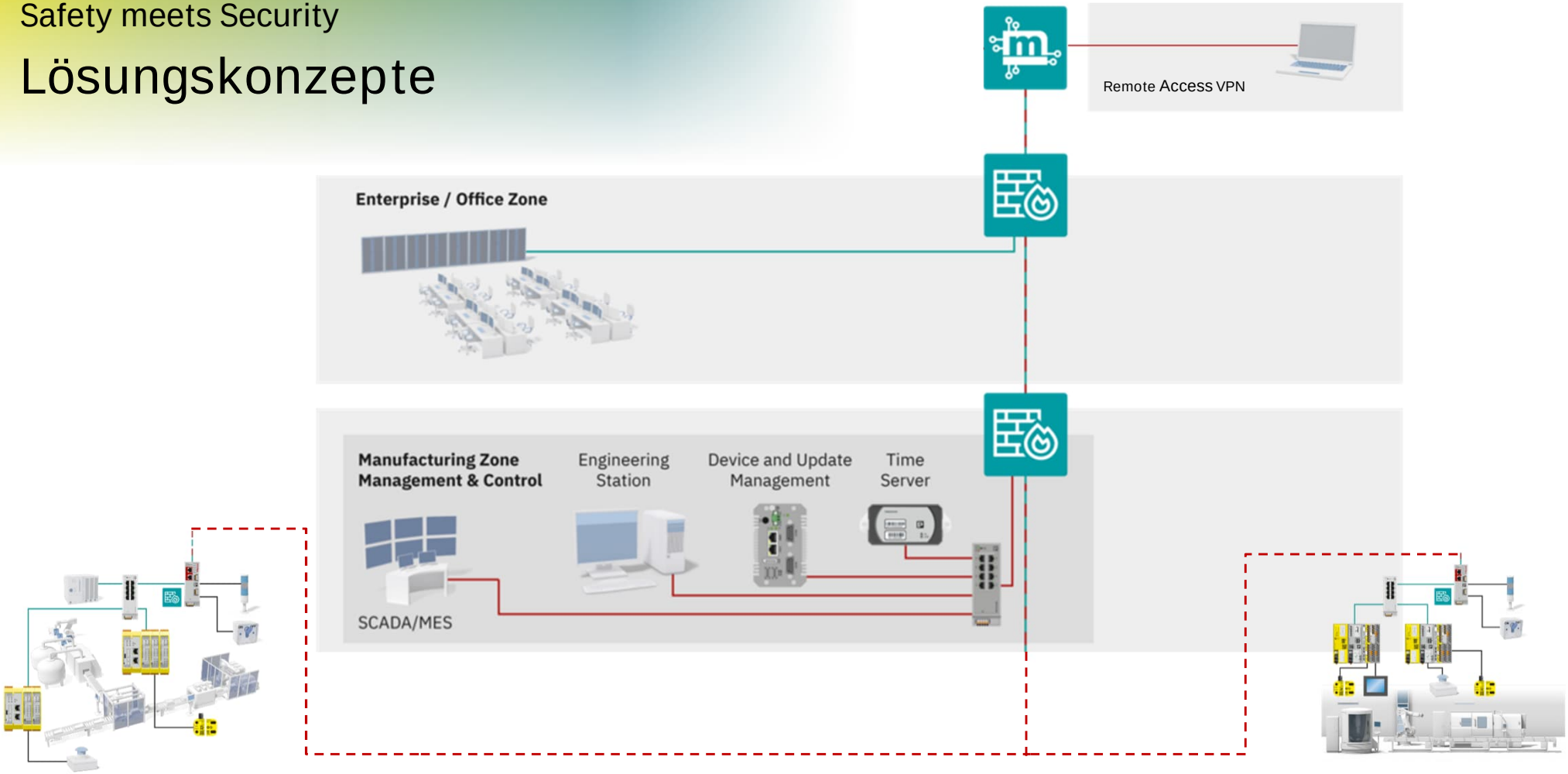
Betreiber



- MVO
  - Wesentliche Veränderung
  - Verkettung von Maschinen
  - Beschaffung von Neuanlagen
- NIS 2
  - Bei Betroffenheit Erfüllung umfangreicher Security-Anforderungen
- CRA
  - Lieferanten werden CRA-konform liefern müssen

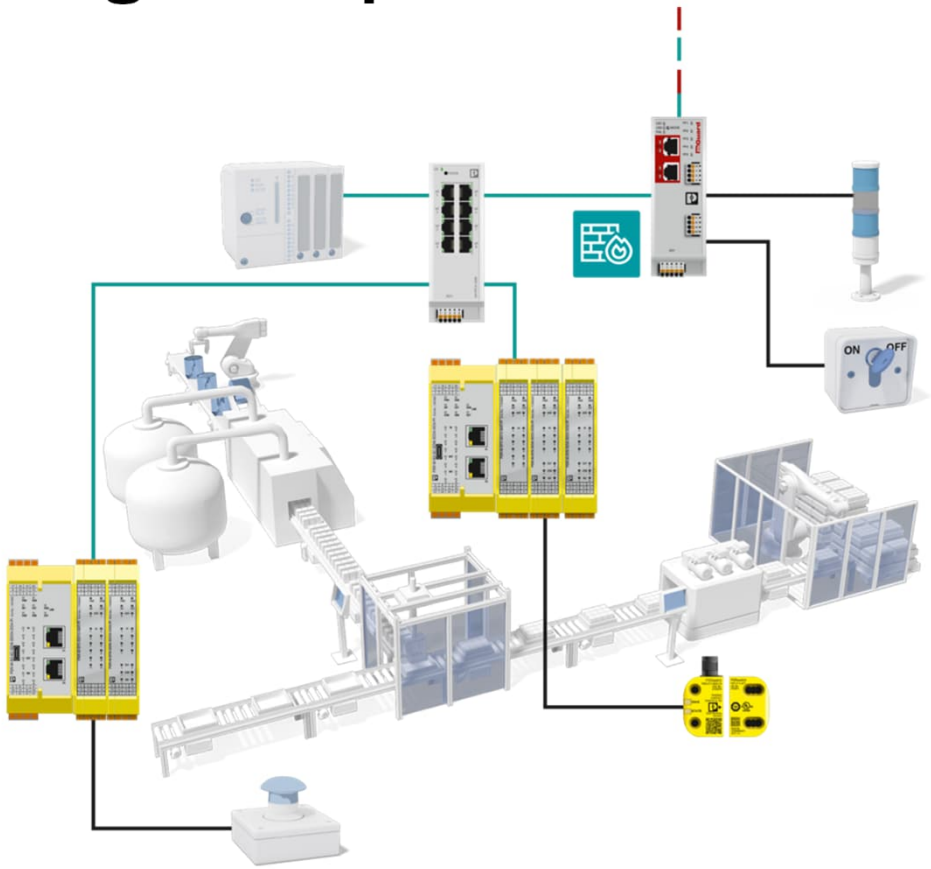
Safety meets Security

Lösungskonzepte



Safety meets Security

Lösungskonzepte

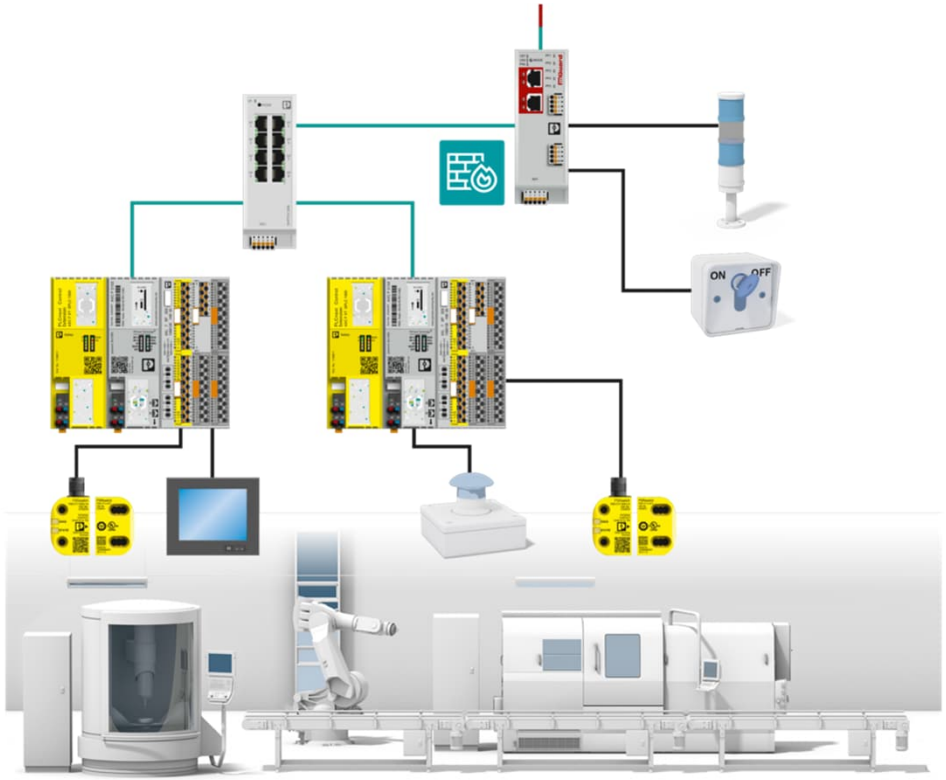


Maschinenlinie 1

- Zonensegmentierung (Defense-in-Depth)
- Zonenabsicherung durch industrielle Firewall
- Kommunikation der Sicherheits-einrichtung innerhalb der Zone mit der Maschinensteuerung
- Zustandskommunikation in übergelagerte Netzwerke
- Sicherer Fernzugriff zur Parametrierung des konfigurierbaren Sicherheitssystems
- VPN-Freigabe durch Schlüsselschalter

Safety meets Security

Lösungskonzepte



Maschinenlinie 2

- Zonensegmentierung (Defense-in-Depth)
- Zonenabsicherung durch industrielle Firewall
- Einsatz Safety SPS mit z.B. Profisafe
- Sicherheitsgerichtete Kommunikation innerhalb der Fertigungslinie
- Zustandskommunikation in übergelagerte Netzwerke
- VPN-Freigabe durch Schlüsselschalter
- Integrierte Security-Maßnahmen auf Gerätebene

Safety meets Security

Wie können wir Sie unterstützen

Umfassendes Produkt- und Lösungsportfolio

- Vom sicheren Sensor bis zur sicheren Steuerung
- Industrielle Firewalls & Netzwerktechnik
- Zeitserver und Device- & Updatemanagement

Vielfältiges Angebot von Seminaren und Schulungen

- Grundlagen der IEC 62443
- CE-Kennzeichnung von Maschinen
- Sicherheitslebenszyklus von Maschinen

Zertifizierte Dienstleistungen

- Konformitätsbewertungsverfahren
- Bedrohungsanalyse
- Anomalieerkennung

all about automation

Besuchen Sie uns an Stand 124

SAFETY meets SECURITY

So gelingt der ganzheitliche Schutz nach MVO, NIS2 & CRA

Thorsten Knöner

PHOENIX CONTACT Deutschland GmbH
Produktmanager SPS und I/O-Systeme