

# SAFETY & SECURITY WACHSEN ZUSAMMEN

Pragmatische Umsetzung von Cyber Resilience Act und neuer  
Maschinenverordnung für den Maschinen- und Anlagenbau



**SVEN SCHWARZER**

Geschäftsführer

- 
- Geschäftsführer Smart Mechatronics
  - Begleitung von Projekten u.a. im Bereich Security
  - Moderation



**DR.-ING. GUDRUN FAY**

Senior Project Manager Security

- 
- Projektleiterin mit Schwerpunkt auf Safety- und Securityprojekten
  - Beratung zu MVO, CRA
  - Langjährige Erfahrung in der Produkt-Zertifizierung



**MARKUS FAHN**

Security Engineer

- 
- Security Engineer mit Fokus auf IoT & Industrial Security
  - Expertise in CRA, RED-DA sowie Normen der industriellen Automation (IEC 62443)
  - Bedrohungsanalyse, Risikobewertung & Security-Konzeption

# Agenda

1. Smart Mechatronics
2. EU Cyber-Regularien: Hintergrund und Vorgehensweisen
3. Hands On – Beispiel zum Vorgehen
4. Q & A





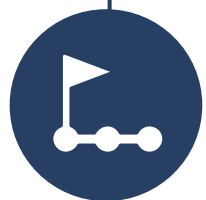
**Mitarbeiter:** 130 +



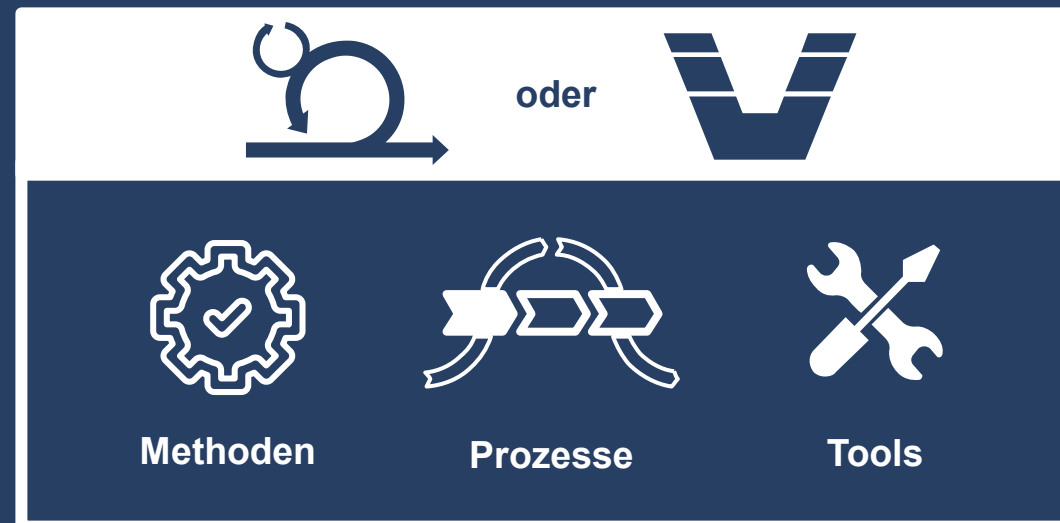
**Standorte:**  
Dortmund, Köln,  
München, Paderborn



**Qualität:**  
Zertifiziert nach  
DIN EN ISO 9001:2015



**Gründung:** 2008



## Engineering

### Embedded Linux

Maßgeschneiderte Embedded Linux Systeme für Ihr Produkt

### RTOS & Firmware

Effiziente Real-Time Operating Systems & Firmware-Entwicklung

### Model Based Engineering

Modellbasierte Softwareentwicklung & Connectivity-Technologien

### Functional Safety

Berücksichtigung aller Aspekte der funktionalen Sicherheit in Ihrem Produkt

### Cybersecurity Engineering

Sichere Produkte & Systeme nach dem Security by Design-Ansatz & CRA

### Testsysteme in der Entwicklung

Individuelle Teststrategien & Prozesse sowie Testautomatisierung

### Low Energy & Energy Harvesting

Energieoptimierte & energieautarke Systementwicklung

### Human Machine Interface

Innovative User Interfaces für einzigartige User Experiences

### Künstliche Intelligenz

Revolutionierung von Entwicklungsprozesse & Produkte

## Beratung

### Entwicklungsmethoden

CONSENS, CONCRY, CONHARD, CONHMI, CONAI  
Proof of Concept

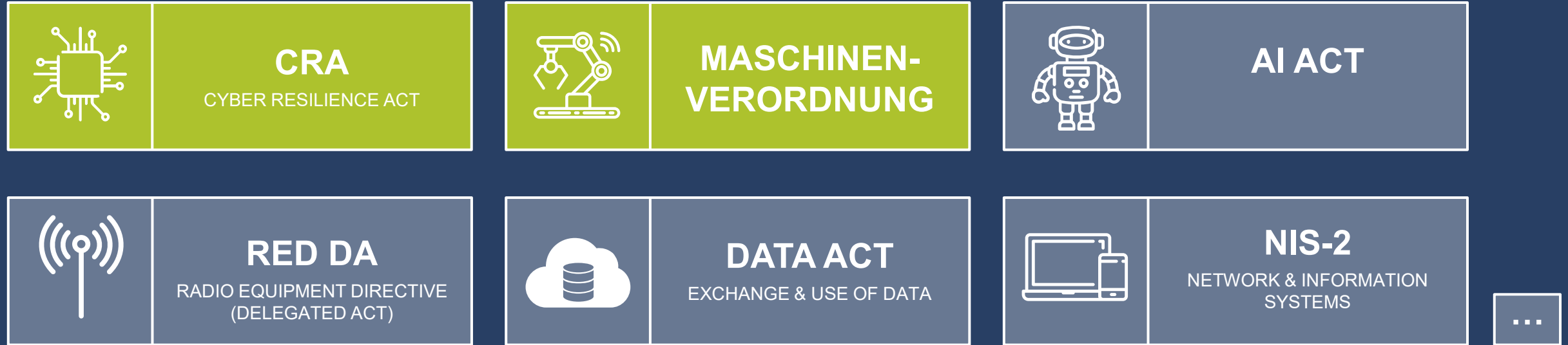
### Prozesse

Security | CRA, RED, Security by Design  
Safety | z.B. ISO26262, IEC 61508

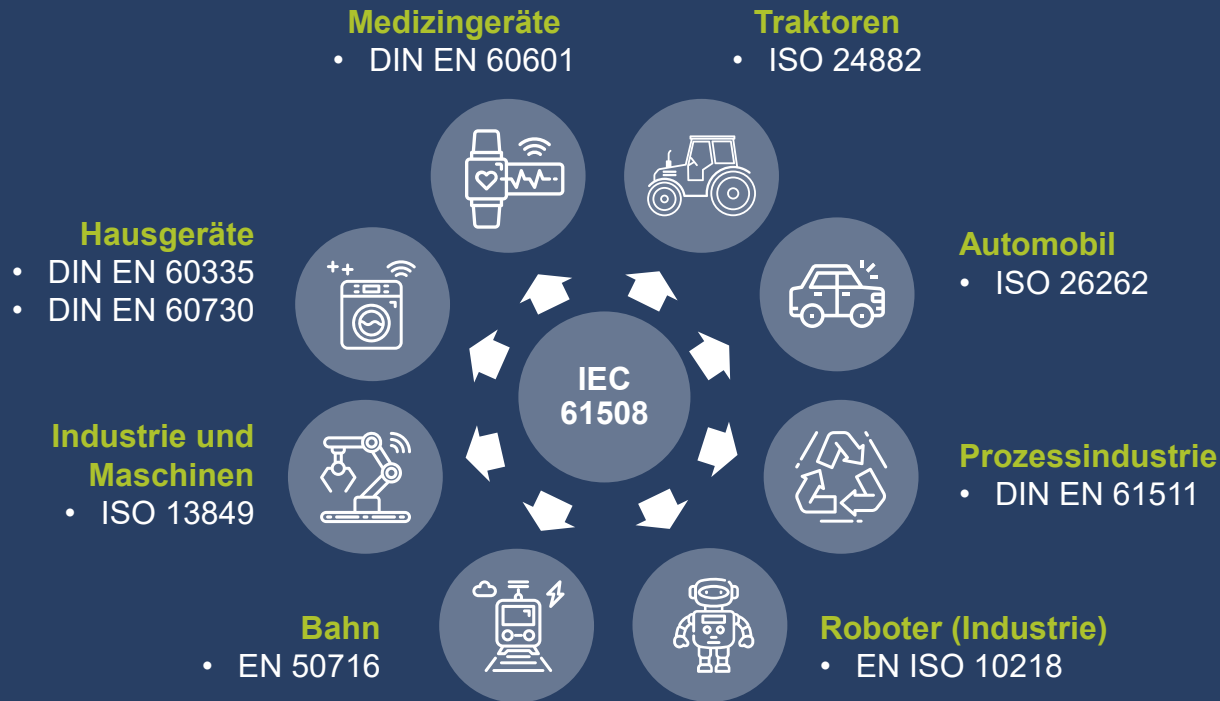
### Tools

Prozessautomatisierung wie CI/CD, SBOM, modellbasierte Entwicklung oder Agentic Workflows

# Übersicht aktueller EU Cyber-Regularien



## Übersicht wichtiger Safety Normen für verschiedene Anwendungsbereiche



### EU Richtlinien/Verordnungen

- *Maschinenrichtlinie*  
2006/42/EG8
- *EU-Maschinenverordnung*  
2023/1230

Die neue MVO trägt der zunehmenden Vernetzung und neuen Techniken, insbesondere KI, Rechnung.

Das hat Auswirkungen auf die Normenlandschaft



### KI

- ISO 21448 – SOTIF
- ISO/IEC TS 22440



### Cyber Security

- ISO 27001
- ISO SAE 21434
- prEN 50742
- IEC 62443

Welche Normen es gibt oder gerade überarbeitet werden, kann im Standardisierungsrequest nachgeschlagen werden.

# Safety-Normen werden überarbeitet

- Übersicht zum Stand der Überarbeitung und Neuentwicklung: [CEN - CENELEC - Search standards](#)

SEARCH IN
 CEN  CENELEC

Keywords

- select a language - ▼

Committee ▼

- Committee -

- Committee title - ▼

Deliverable

Type ▼

- Deliverables -

Standard Reference

Legal Framework ▼

2023/1230 (MACHINERY\_2023)

Status

Preliminary Stage  
  Under Draft  
  Under Approval (  Under Enquiry )  
  Approved  
  Published  
 Withdrawn

Standards Classification

ICS ▼

- ICS -

Activity sector ▼

- Activity Sectors -

Sustainable Development Goals (SDGs) ▼

- SDG -

RESET

SEARCH

Welchen Stand hat "meine" Norm?

# Änderungen der MVO gegenüber der Maschinenrichtlinie

Aspekt	Maschinenrichtlinie (2006/42/EG) – gültig bis 19.01.2027	Maschinenverordnung (EU 2023/1230) – gültig ab 20.01.2027	Änderungen
Sicherheitsanforderungen	Formuliert allgemeine Sicherheitsgrundsätze	Stellt erweiterte, präzisere Anforderungen an Risikoanalyse und -bewertung	<ul style="list-style-type: none"> <li>MVO definiert schärfere Bestimmungen zur Risikoanalyse und Bewertung.</li> <li>Die Verordnung verlangt detailliertere und umfassendere Verfahren zur Risikobewertung.</li> </ul>
Neue Technologien	Keine spezifische Regelung zu KI, vernetzten Systemen etc.	Bezieht neue Technologien wie KI explizit ein und definiert Anforderungen zur Risikominimierung	<ul style="list-style-type: none"> <li>In der Verordnung werden neue Technologien wie künstliche Intelligenz (KI) und vernetzte Systeme berücksichtigt.</li> </ul>
Hochrisikomaschinen	Keine gesonderte Kategorisierung	Einführung der Kategorie „Hochrisikomaschinen“ mit strengeren Prüfverfahren und Drittstellenbeteiligung	<ul style="list-style-type: none"> <li>Einführung einer Kategorie von Hochrisikomaschinen. Solche Maschinen müssen zusätzlich von Dritten überprüft werden.</li> </ul>
Cybersicherheit	Keine Regelung	Anforderungen zum Schutz vor Cyberangriffen auf Steuerungssysteme	<ul style="list-style-type: none"> <li>Neue Anforderungen an die Cybersicherheit von Maschinen und deren Steuerungssysteme. Hersteller müssen sicherstellen, dass Maschinen gegen Cyberbedrohungen geschützt sind.</li> </ul>
Verantwortlichkeiten der Hersteller	Allgemeine Anforderungen	Präzisiert Pflichten zu Rückverfolgbarkeit und Sicherheitsüberwachung über den Lebenszyklus	<ul style="list-style-type: none"> <li>Die Verordnung präzisiert die Verantwortlichkeiten der Hersteller in Bezug auf die Nachverfolgbarkeit und Überwachung der Sicherheit von Maschinen im gesamten Lebenszyklus.</li> </ul>
Strafmaßnahmen	Strafmaßnahmen obliegen den Mitgliedstaaten	Einheitliche Vorgaben auf EU-Ebene, inkl. Rückruf gefährlicher Maschinen	<ul style="list-style-type: none"> <li>MVO enthält spezifische Bestimmungen über Strafmaßnahmen bei Nichteinhaltung, einschließlich der Möglichkeit unsichere Maschinen aus dem Verkehr zu ziehen.</li> </ul>

# Schutzziele der MVO: Safety einschließlich Security



Die Schutzziele der MVO umfassen den Schutz von Systemen und Daten vor Cyberangriffen

# Schutzziele der MVO und des CRA

## Safety (klassisch)

Technisches Versagen

Fehlerhafte Implementierung (Bug)

Falsches Design

(Berücksichtigt eine) bekannte  
Produktumgebung

## Security MVO (Schutz des Produkts)

Böswillige Manipulation digitaler Elemente

Angriffe vom Netzwerk

Malware

Manipulierte Kommunikation

DoS-Attacken

Fehlerhafte Implementierung (Vulnerability)

## Security CRA (ganzheitlich)

Angriffe aufs Netzwerk

Abgehörte Kommunikation

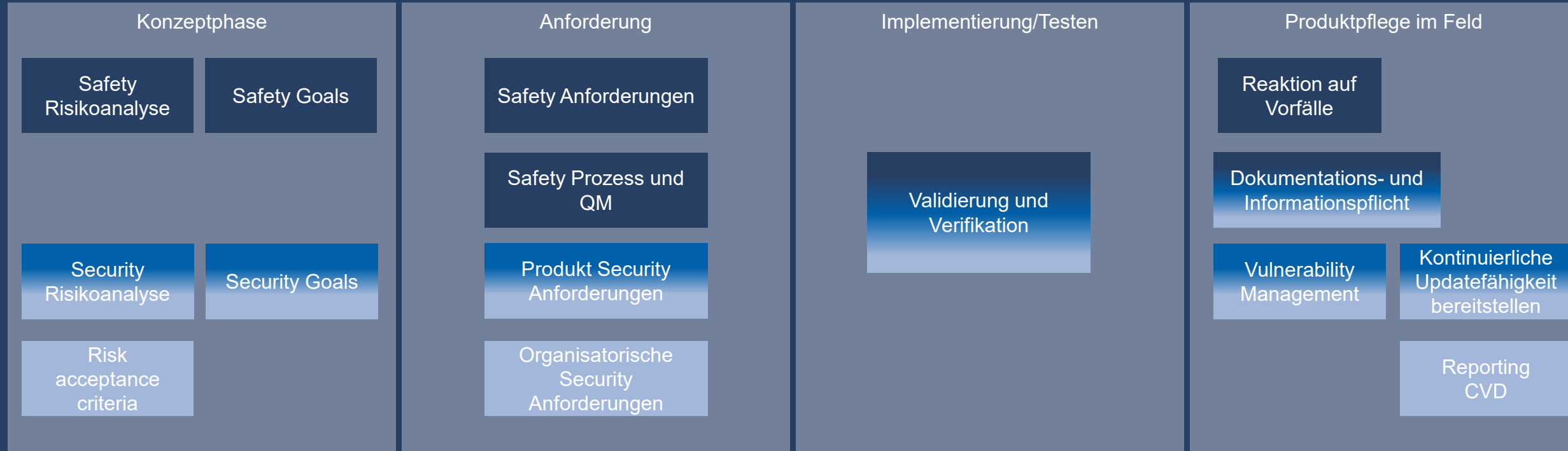
Datenschutz

Schutz von IP

Schutz der Infrastruktur

Die Schutzziele des CRA gehen über den Betrachtungsbereich der MVO hinaus und schließen die digitale Umgebung ein

# Erweiterung des Safety Produkt-Lifecycle durch Security



MVO Safety

MVO Security

CRA

Safety schützt Menschen und Umwelt vor physischen Schäden  
Security erweitert dies um die Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit

# Mapping der Anforderungen von CRA und MVO

## MVO

Essential Health and Safety Requirements

Behördenzugriff auf Source Code

In der MVO gelten strengere Anforderungen an die Produktintegrität als beim CRA

## Gemeinsame Anforderungen

Secure-by-Design

Logging Security-relevanter Ereignisse

Vorgaben zur Anleitung für Nutzer

Vorgaben zur technischen Dokumentation

CVE (z. B. SBOM)

Aufbewahrungspflichten

Risikomanagement

Produktanforderungen (Integrität)

Vorgaben zur Konformitätsbewertung

Security Updates

Schwachstellenmanagement

## CRA

Produktanforderungen (Vertraulichkeit, Verfügbarkeit)

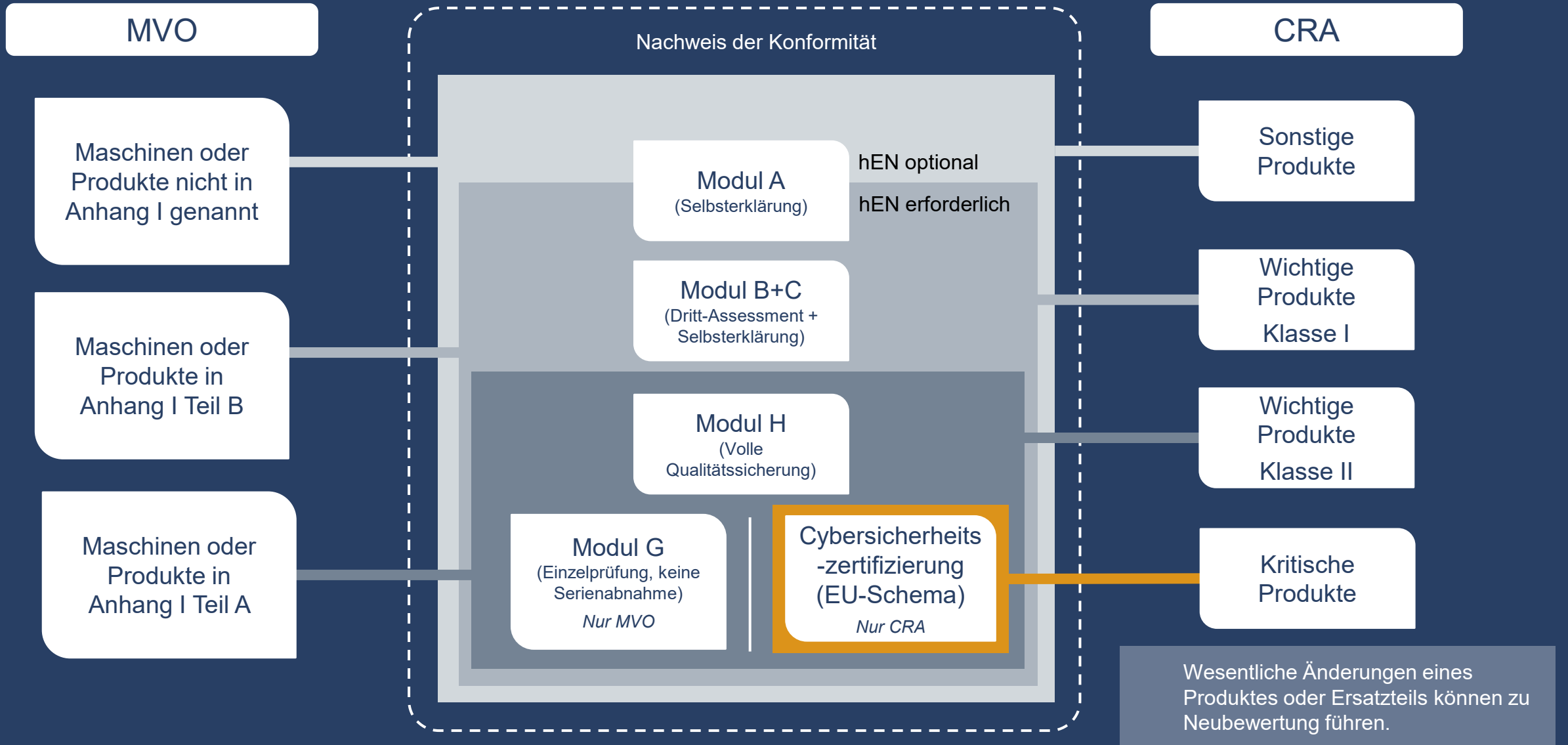
Festgelegter Unterstützungszeitraum

Meldepflichten

SBOM

Im CRA strenger geregelt.

# Der Weg zum CE-Kennzeichen: Konformitätsbewertung nach CRA und MVO



Vereinfachte Darstellung

# Beispiel – Metallpresse

CRA Relevant

Verwendet in Innenräumen in einer Industrieanlage zum Pressen von Metallteilen.

HMI (Touch Panel)

Standard PLC

PC zur Wartung (zeitweise verbunden)

Vertraulichkeit  
VNC-Zugangsdaten

Industrial Ethernet Switch

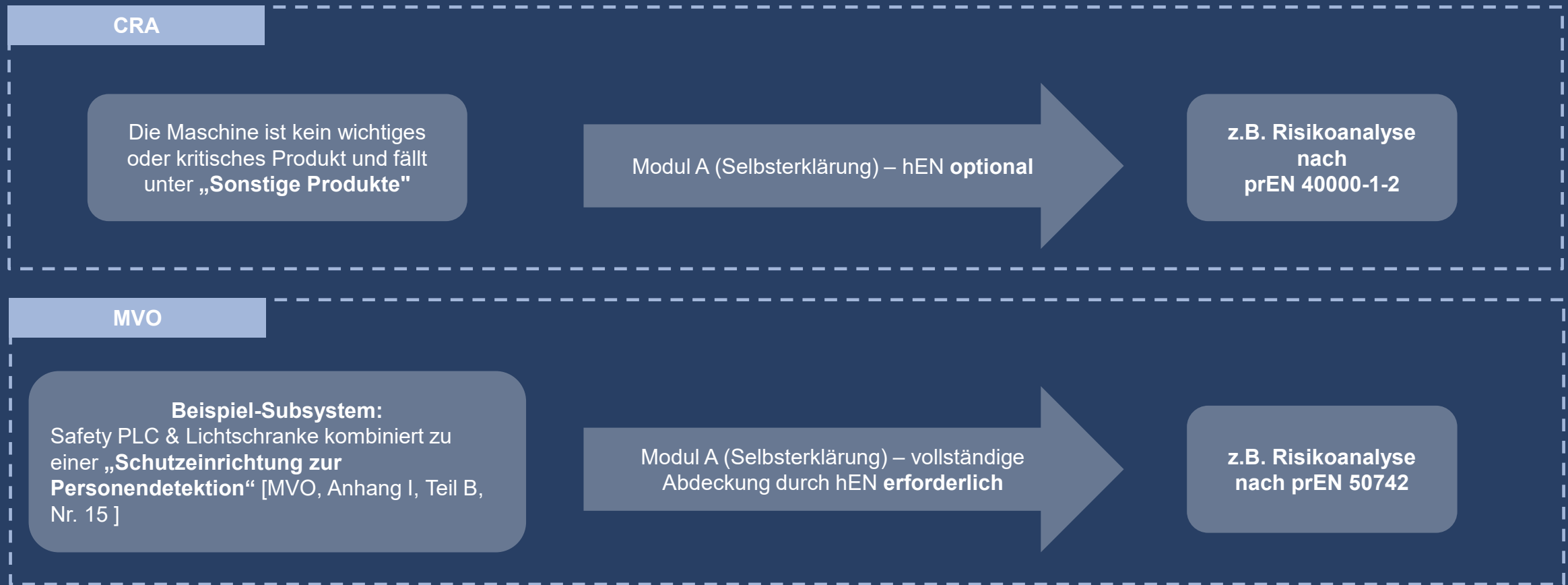
Safety PLC

Safety I/O Module

Lichtschranke

Integrität  
Sichere Press-Stop-Konfiguration

Safety Zone



Bezüglich der MVO gilt:  
Bestimmte Konformitätsbewertungsverfahren können auf Subsysteme der Maschine angewandt werden

# Beispiel zur Risikoberechnung nach prEN 50742 – Metallpresse

Setzt auf der Risiko  
Bewertung nach ISO 12100  
auf – Safety-Maßnahmen

## Security Asset mit Safety-Relevanz: Sichere Press-Stop-Konfiguration

## Security Asset ohne Safety-Relevanz: Zugangsdaten - Fernwartung

1.

### SECURITY- KONTEXT BESTIMMEN

Lichtschanke, Bus-Leitung und Safety PLC sind frei zugänglich

VPN-Tunnel endet am Maschinennetzwerk. Keine Brute-Force-Protection.

2.

### THREATS IDENTIFIZIEREN

Threat: Tampering  
Einstellung an der Safety PLC wird verändert → Lichtschanke wird ignoriert

Threat: Information Disclosure  
VNC-Passwort ist in der Länge limitiert und kann in realistischer Zeit erraten werden

3.

### RISIKO ABSCHÄTZEN

Safety Related Security Level:  
**SRSL1**

Safety Related Security Level:  
**Nicht Anwendbar**



Der Security Impact ist nicht im Scope der Norm!

4.

### RISIKO- BEHANDLUNG

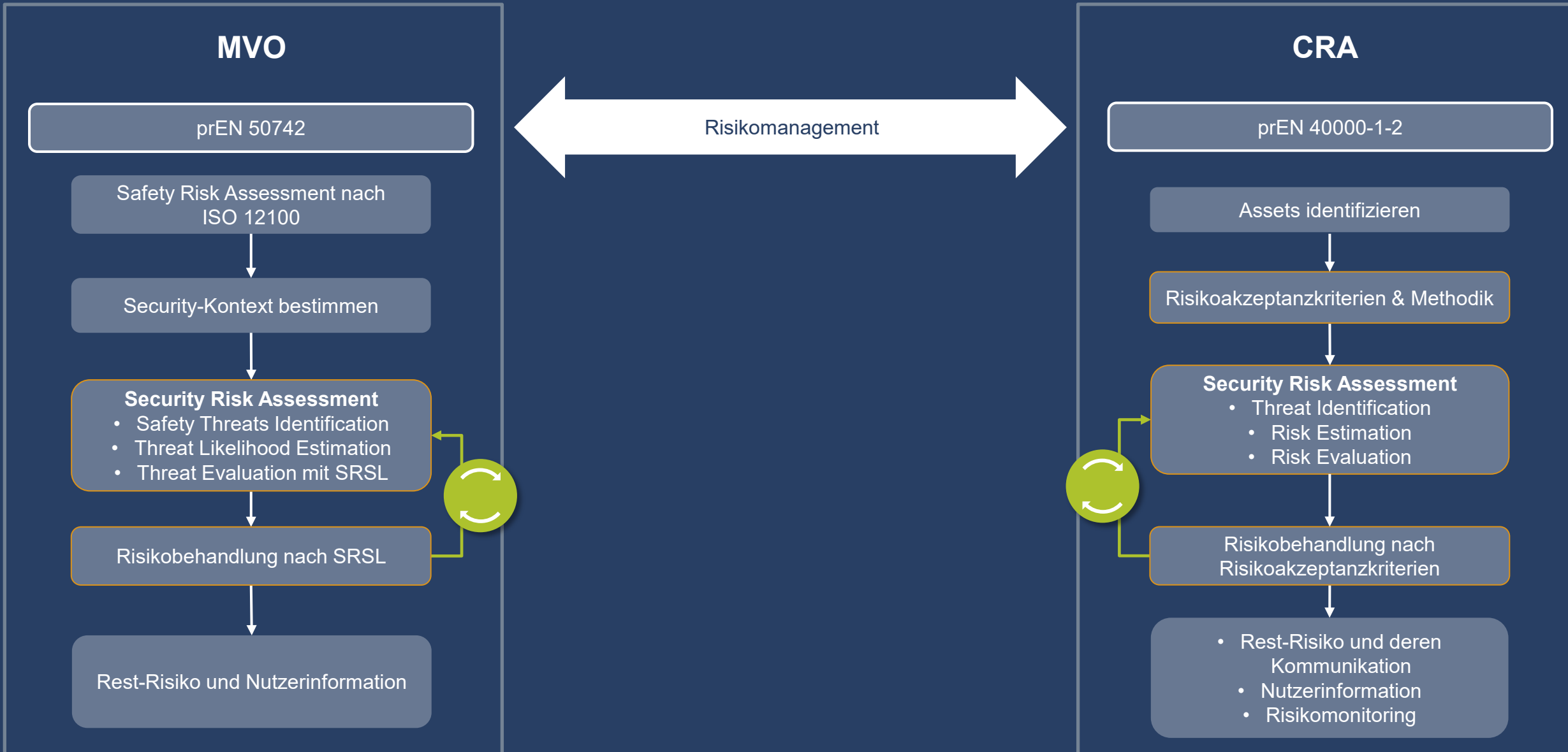
Nach prEN50742 – Mechanismen zur Authentifikation und zum Schutz der Integrität müssen ergänzt werden

Keine Mechanismen in der prEN50742 sind hier sinnvoll anwendbar.

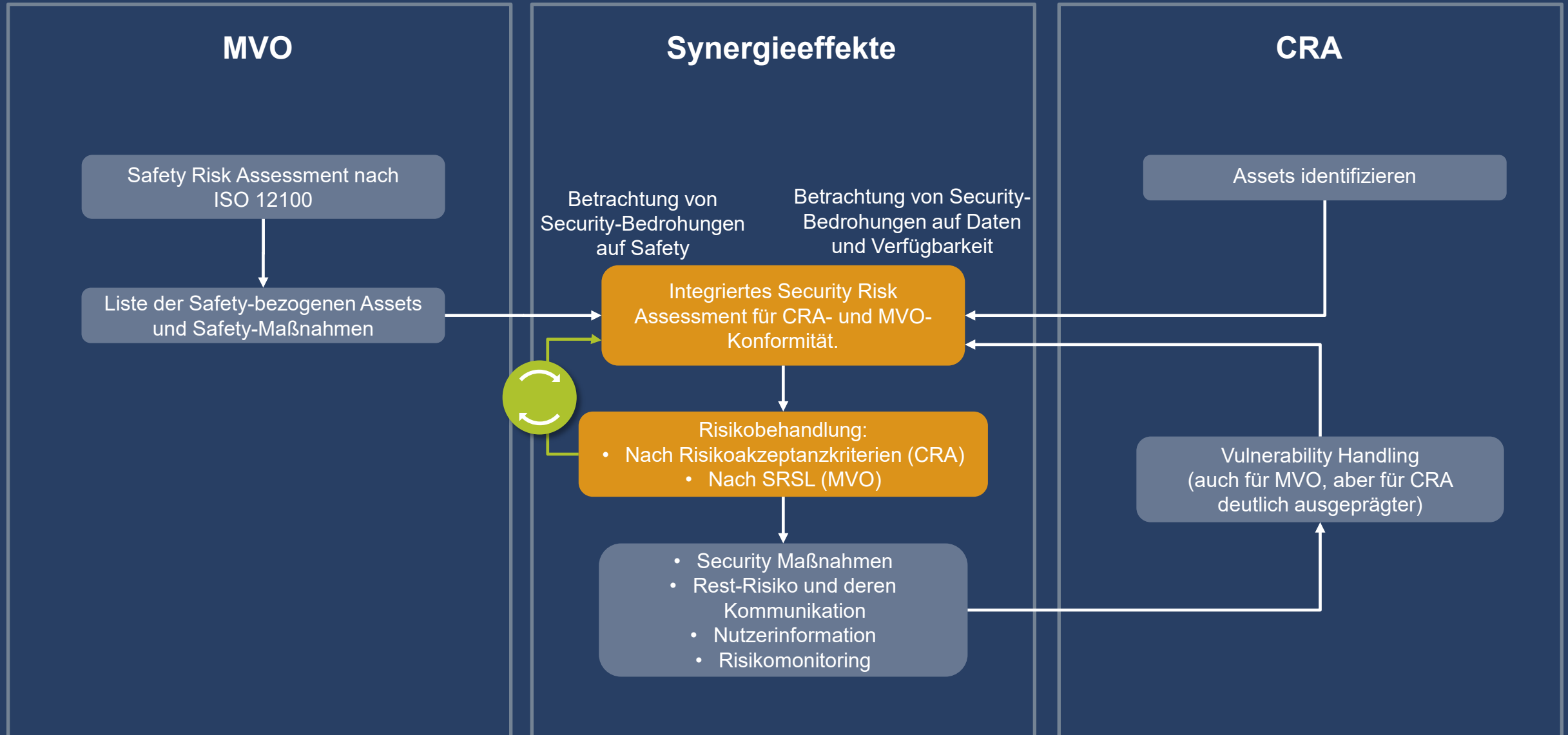


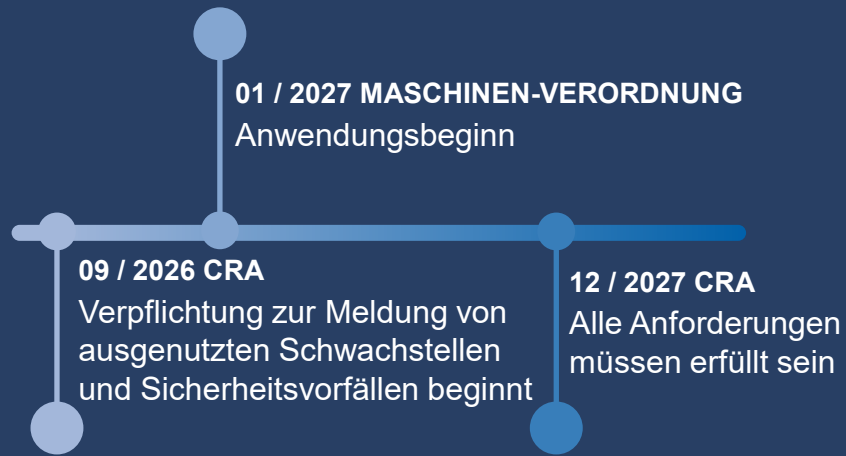
Die Maßnahmen sind nicht anwendbar, zur Mitigation dieser Bedrohung.

# Risikomanagement für CRA und MVO getrennt



# Nutzen von Synergien





MVO kommt, Hersteller müssen sich damit auseinandersetzen

CRA ≠ MVO, **aber** Synergien können Mehraufwand minimieren

Die strukturierte und vereinheitlichte Risikoanalyse ist der Schlüssel zur effizienten Erfüllung beider Verordnungen

**NOCH FRAGEN?  
Dann kontaktieren Sie uns gerne!**

[www.smartmechatronics.de](http://www.smartmechatronics.de)



**Sven Schwarzer**

Geschäftsführer

T +49 231 841685-110

M +49 160 95654194

[sven.schwarzer@smartmechatronics.de](mailto:sven.schwarzer@smartmechatronics.de)



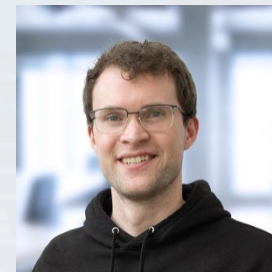
**Dr.-Ing. Gudrun Fay**

Sen. Project Manager Security

T +49 231 841685-232

M +49 151 25783975

[gudrun.fay@smartmechatronics.de](mailto:gudrun.fay@smartmechatronics.de)



**Markus Fahn**

Security Engineer

T +49 231 841685-278

M +49 151 62831607

[markus.fahn@smartmechatronics.de](mailto:markus.fahn@smartmechatronics.de)