



► Cyber Security & CE Herausforderungen durch MVO & CRA

Weltnormentag 2026, WKO NÖ
Maximilian Traxler, 14.10.2026

PILZ
THE SPIRIT OF SAFETY

► Agenda

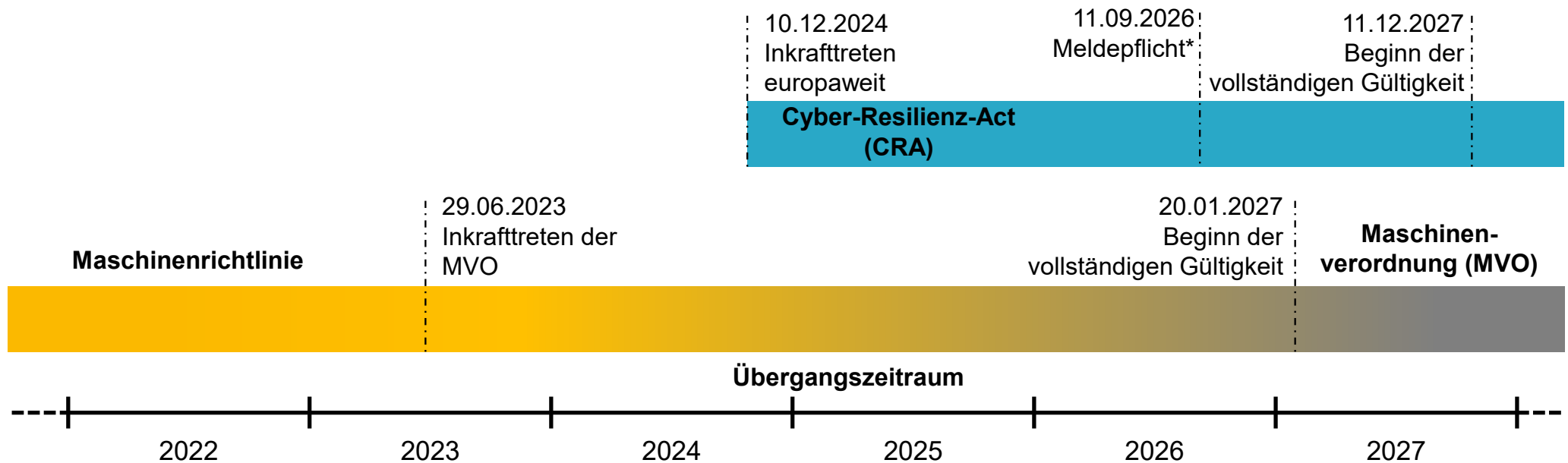
- 01** ► Kurzer Überblick zu den Anforderungen
- 02** ► prEN 50742: Die norm der Security in der MVO
- 03** ► CRA & MVO parallel erfüllen?
- 04** ► Zusammenfassung

01

- ▶ Kürzer Überblick:
Gesetzliche Anforderungen

► Kurzer Überblick: Gesetzliche Anforderungen

Zeitleiste



1.1

- ▶ Maschinenverordnung (EU)
2023/1230

► Maschinenverordnung (EU) 2023/1230

Anhang III – Grundlegende Gesundheits- und Sicherheitsanforderungen

- Schutz vor vorsätzlicher und unbeabsichtigter Manipulation.
- Cyberbedrohungen sind ausdrücklich mit Gesundheits- und Risiken der Sicherheit verbunden sind.
- Security-Mängel werden als potenzielle Sicherheitsmängel behandelt, wenn sie zu einer gefährlichen Situation führen können.



**Cybersicherheit
als Safety-
Anforderung**

► Maschinenverordnung (EU) 2023/1230

Anhang III, Abschnitt 1.1.9

- Bezieht sich nur auf das Safety-System
- Netzwerke, Schnittstellen oder Geräteanschlüsse dürfen keine neuen Gefahren verursachen.
- Der Entwurf muss die Erkennung folgender Ereignisse ermöglichen:
 - unbefugter Zugriff.
 - vorsätzliche oder unbeabsichtigte Manipulation.




**Schutz gegen
Korrumpierung**

► Maschinenverordnung (EU) 2023/1230

Anhang III, Abschnitt 1.2.1 (a), (f)

- Beständigkeit gegen Betriebsbeanspruchungen
 - Steuerungssysteme müssen den vorgesehenen Betriebsbelastungen und vorhersehbaren außergewöhnlichen Bedingungen standhalten.
- Rückverfolgbarkeit von Änderungen an Software zur Sicherheit:
 - Änderungen an Software zur Sicherheit müssen aufgezeichnet und rückverfolgbar sein.



**Sicherheit und
Zuverlässigkeit
von
Steuerungs-
systemen**

1.2

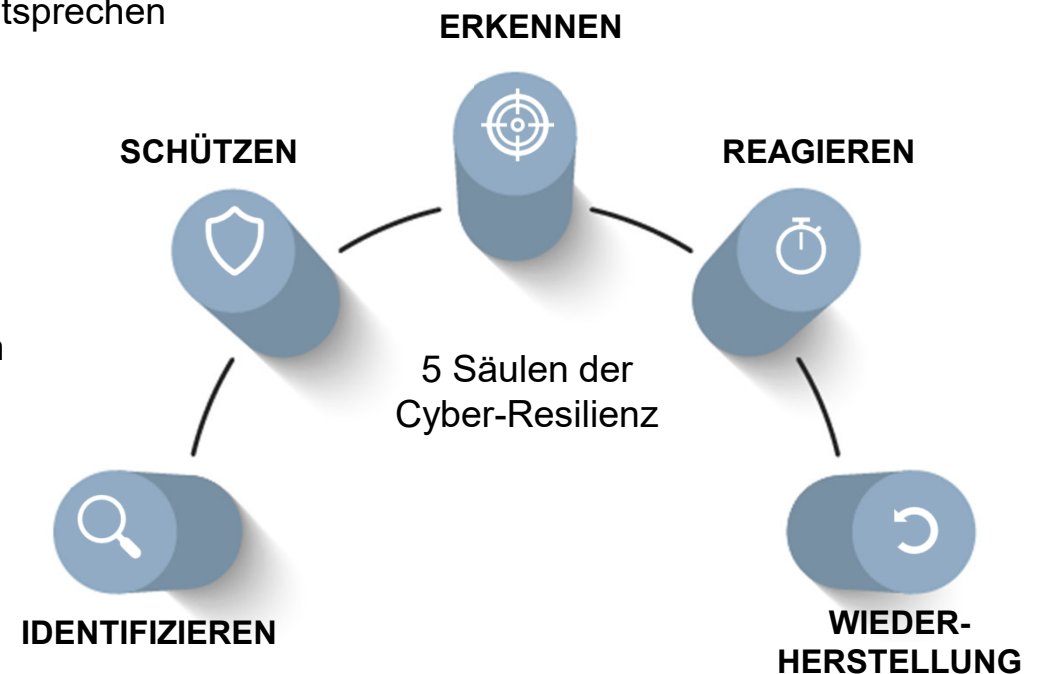
- ▶ Cyber Resilience Act (EU)
2024/2847

► Cyber Resilience Act (CRA)

Anwendung

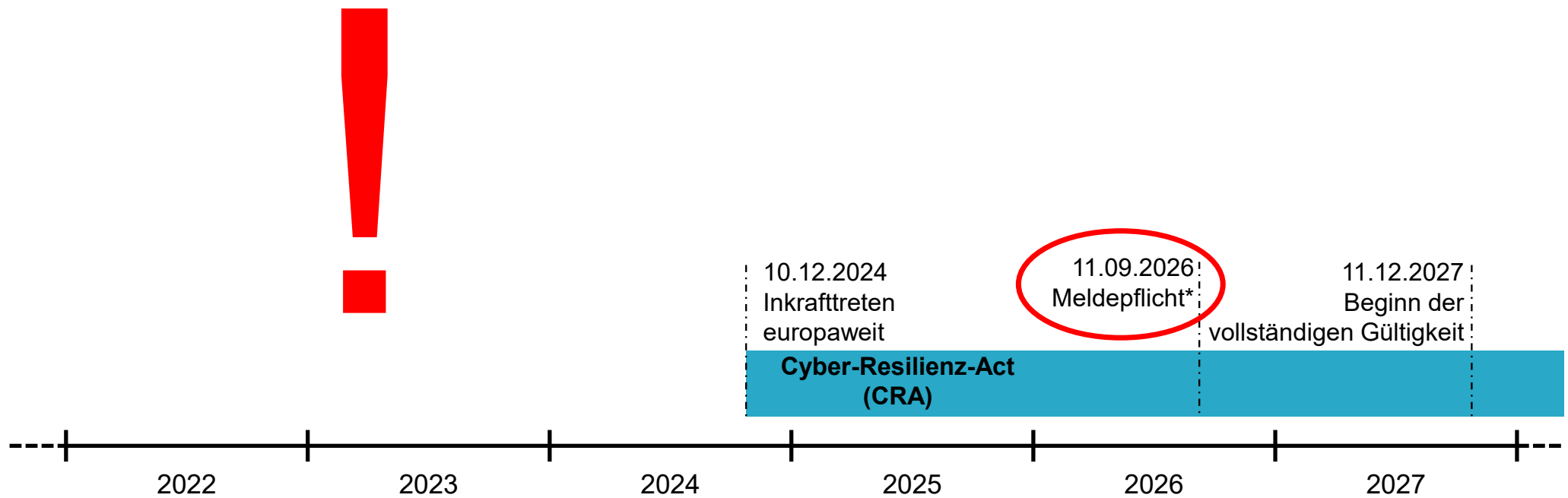
- Konzipieren, Entwickeln und Herstellen von digitalen Produkten mit einem angemessenen Cybersicherheitsniveau
- Dazu kann eine **Risikobeurteilung** verwendet werden.
Alle Produkte müssen den grundlegenden Anforderungen entsprechen und sind mit einer CE-Kennzeichnung zu versehen:
 - **Secure by Design**
 - **Vorbereitung auf Sicherheitsvorfälle**
 - **Verwaltung von Schwachstellen**
- Verbesserung der Transparenz von Sicherheitsinformationen
- Bereitstellen von Updates und Informationen

Hinweis: Produkthersteller sollten die Anforderungen des CRA **bereits heute** umsetzen, um die Gewährleistung der Konformität in Zukunft (11.12.2027) gewährleisten zu können.



► Cyber Resilience Act (CRA)

Zeitleiste



► Cyber Resilience Act (CRA)

Behandlung von Schwachstellen

- Schwachstellen der Komponenten meines Produkts sollen in einer **Software Bill of Material (SBOM)** festgehalten werden
- Melden einer ausgenutzten Schwachstelle meines Produkts an ENISA und nationalem CSIRT über die Meldeplattform:

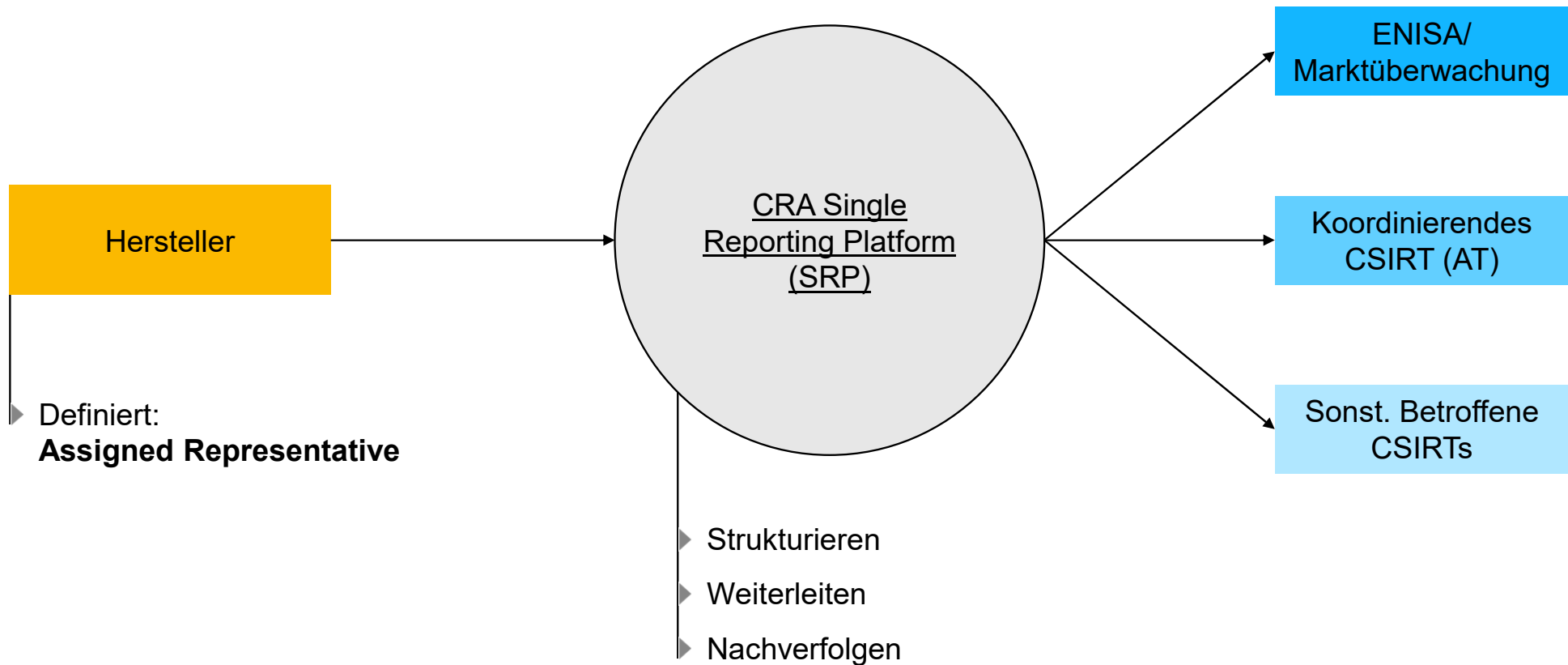


- Die Kunden müssen ebenfalls informiert werden → CSAF-Format
- Security-Updates sollen getrennt von Funktionsupdates ausgeliefert werden
- Der Prozess für Behandlung der Schwachstellen muss dokumentiert sein

NEW

► Cyber Resilience Act (CRA)

Single Reporting Platform



► Cyber Resilience Act (CRA)

Zusammenfassung



CE EU-Konformitätserklärung

Konformitätserklärung gemäß
2024/2847 Anhang V oder VI

Konformitätsbewertungsverfahren
2024/2847 Anhang VIII

Interne Kontrolle
Modul A

Bewertung durch Dritte
Modul B+C, Modul H oder
EU-Cybersicherheits-
zertifizierung



Technische Dokumentation

Berichte über die durchgeführten
Prüfungen

Bewertung der
Cybersicherheitsrisiken im
Lebenszyklus

Prozess zum Umgang mit
Schwachstellen

Sicherheitsrisikobeurteilung

Cybersicherheitslösung



Anleitung für Nutzer

**Auszüge aus der technischen
Dokumentation 2024/2847 Anhang II**

- Verwendungszweck
- Wesentliche Funktionen
- Supportzeitraum, Ansprechpartner
- So installieren Sie Updates
- SBOM (falls zutreffend)
- Vorhersehbare Umstände, Missbrauch oder Änderungen, die zu Risiken führen können.
- Wie die Standardeinstellung für Updates deaktiviert werden kann
- Informationen für den Integrator

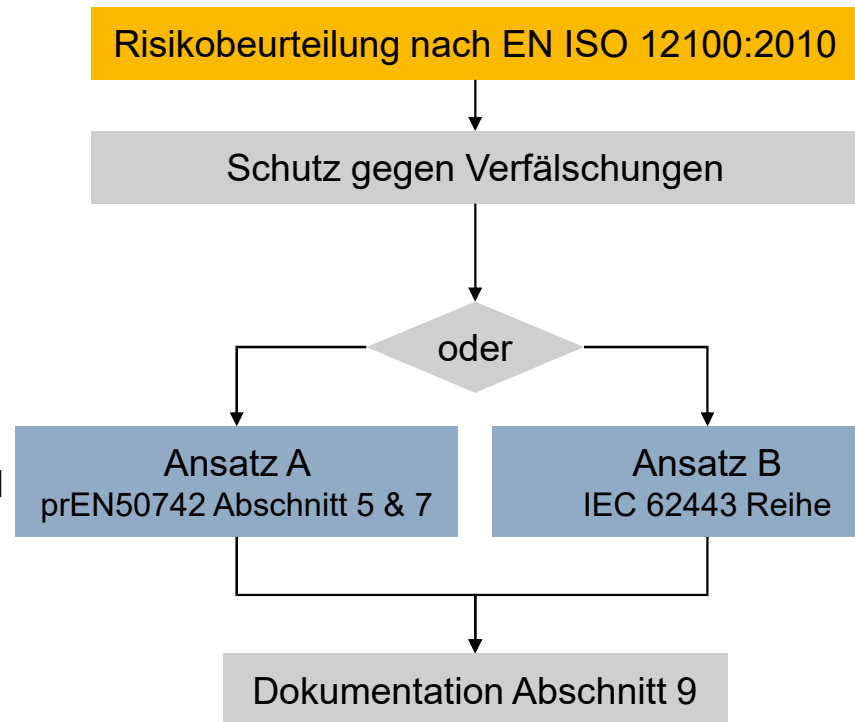
02

- ▶ prEN 50742:
Die norm der Security in der
MVO

► Schutz gegen Korrumpierung

prEN 50742 – Allgemeine Verfahrensanforderungen

Grundlegende Anforderungen
und Empfehlungen zur
Verhinderung einer zufälligen und
vorsätzlichen (einschließlich
böswilligen) Verfälschung von
Maschinen, die zu gefährlichen
Situationen führt, zu erfüllen
→ **Ansatz A**



Wenn hingegen bevorzugt für die
Sicherheitsanforderungen der
Maschinen eher die Normen
EN IEC 62443-3-3:2019
EN IEC 62443-4-1:2018
EN IEC 62443-4-2:2019
zu befolgen
→ **Ansatz B**

► Approach A: Threat Assessment

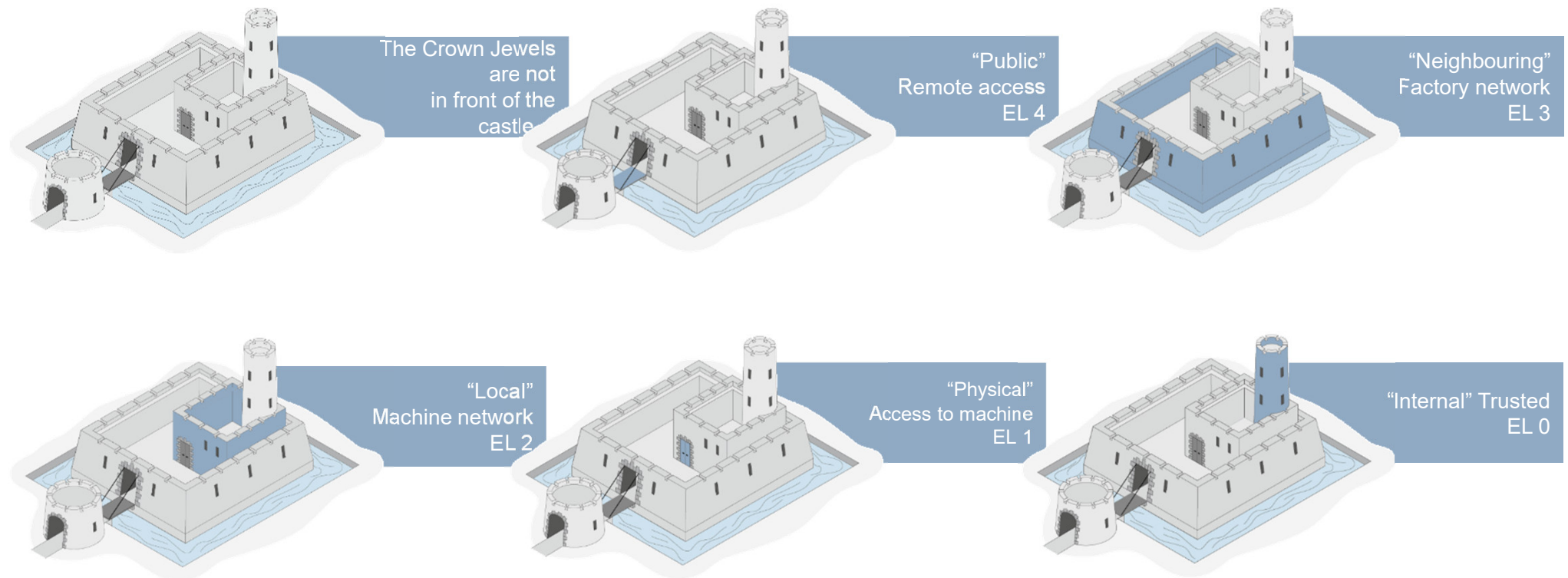
prEN 50742

$$AP = EL \times WoO + AC$$

- AP ... Attack potential
- AC ... attacker's capability (Komplexität) Werte: 1 | 2 | 3 | 4
- WoO ... Window of opportunity (für eine Maschine im Security-Kontext) Werte: 0.6 | 0.8 | 0.9 | 1
- EL ... **exposure level** (pro Schnittstelle, pro Verbindung) Werte: 0 | 2 | 5 | **16** | **24**

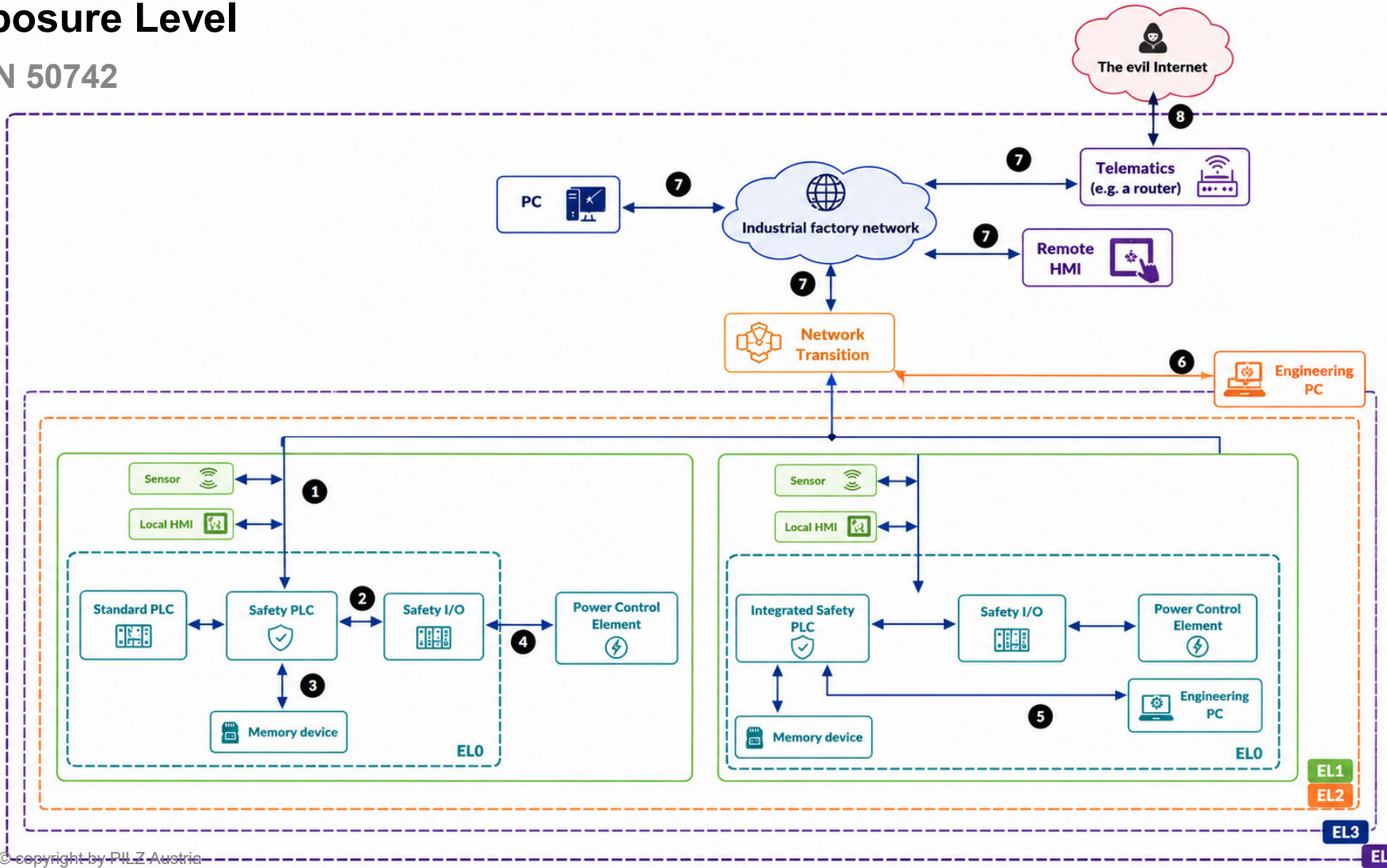
► Approach A: Threat Assessment

Exposure Level



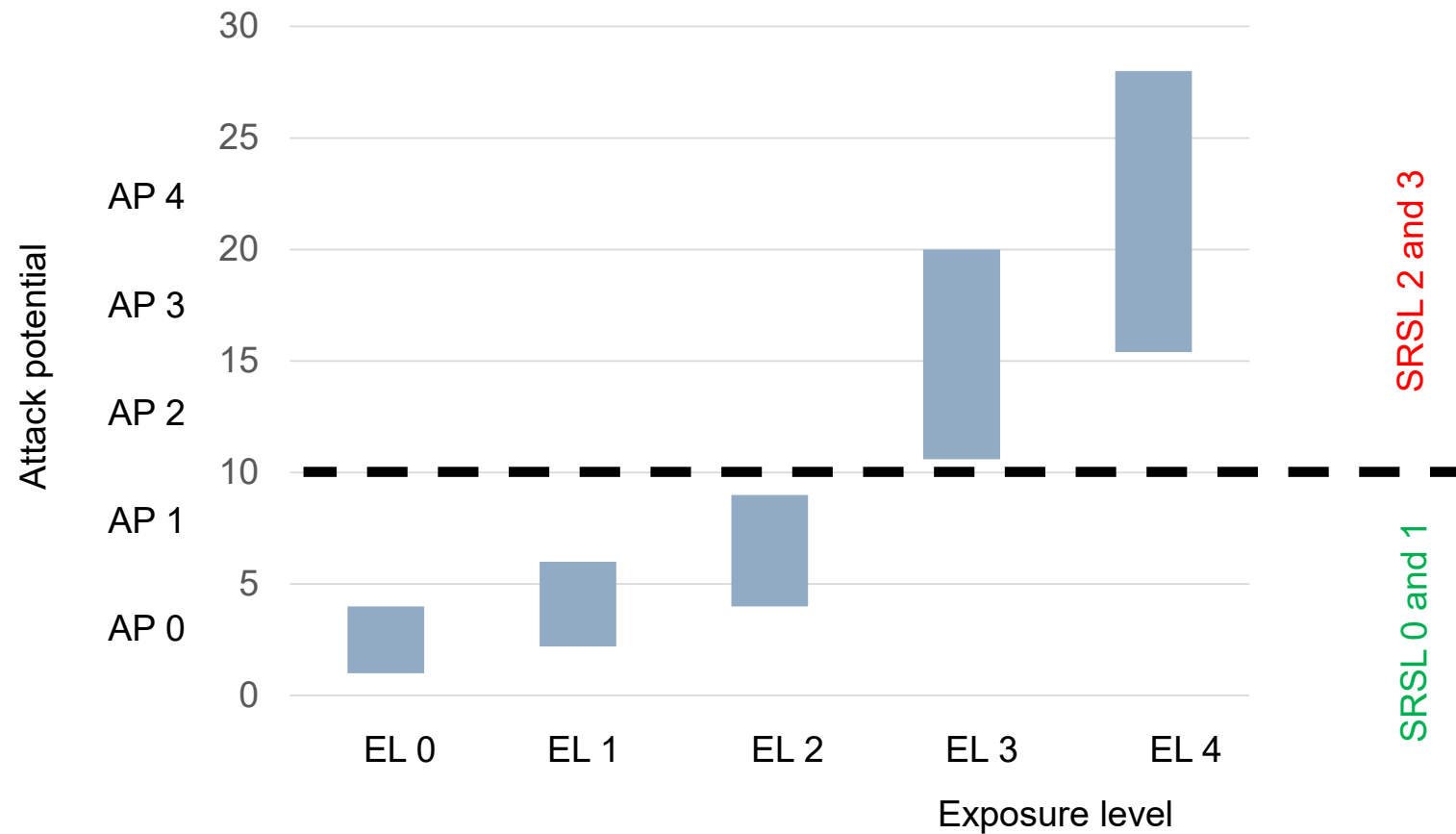
▶ Exposure Level

prEN 50742



► Übersicht zum SRSL

Der Schlüssel ist die Erreichbarkeit



Schaden	
Reversibel	Irreversibel
SRSL 3	SRSL 3
SRSL 2	SRSL 3
SRSL 1	SRSL 2
SRSL 1	SRSL 1
SRSL 0	SRSL 0

03

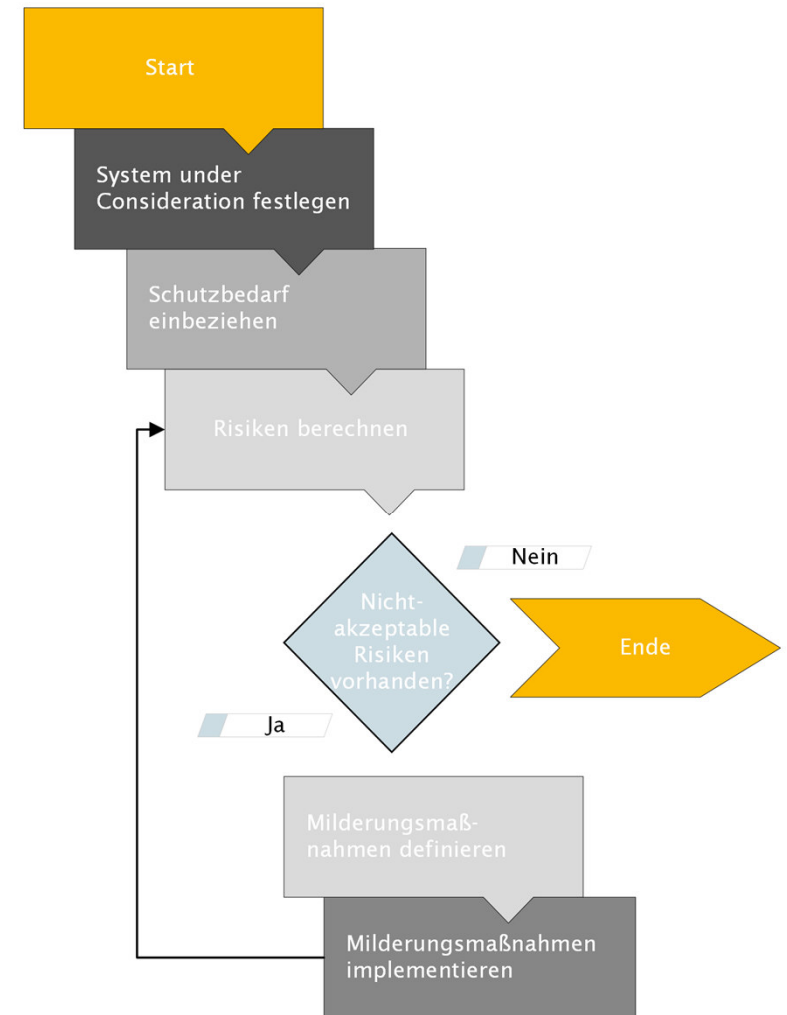
- ▶ CRA & MVO parallel erfüllen?

► Eine Risikobeurteilung, 2 Gesetze

► Folgende Dokumente beschreiben solche Prozesse:

- IEC 62443-3-2
- IEC 62443-2-1
- ISO 27001
- BSI ICS-Security-Kompendium
- NIST SP 800-82
- ...

► Sehr breit formuliert → es gibt (zum jetzigen Stand) kein Kochrezept



► Eine Risikobeurteilung, 2 Gesetze

► 2 unterschiedliche Ziele

- Securer Betrieb der Maschine (Ausfallsicherheit, Datensicherheit, ...)
- Safety Secure gestalten

► Kritische Komponenten für Safety und den Betrieb werden separat bestimmt



Schutzbedarf
einbeziehen



► Security By Desing

CRA-Anhang 1 – Basierend auf den Cyber-Security-Risiken



04

► Zusammenfassung

► Zusammenfassung

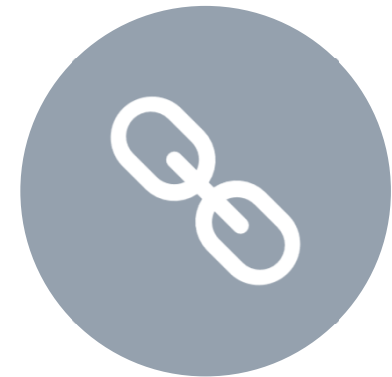
Anforderungen an Produkte/Hersteller → CRA & MVO



Fragen Sie Lieferanten nach
deren CRA-Status



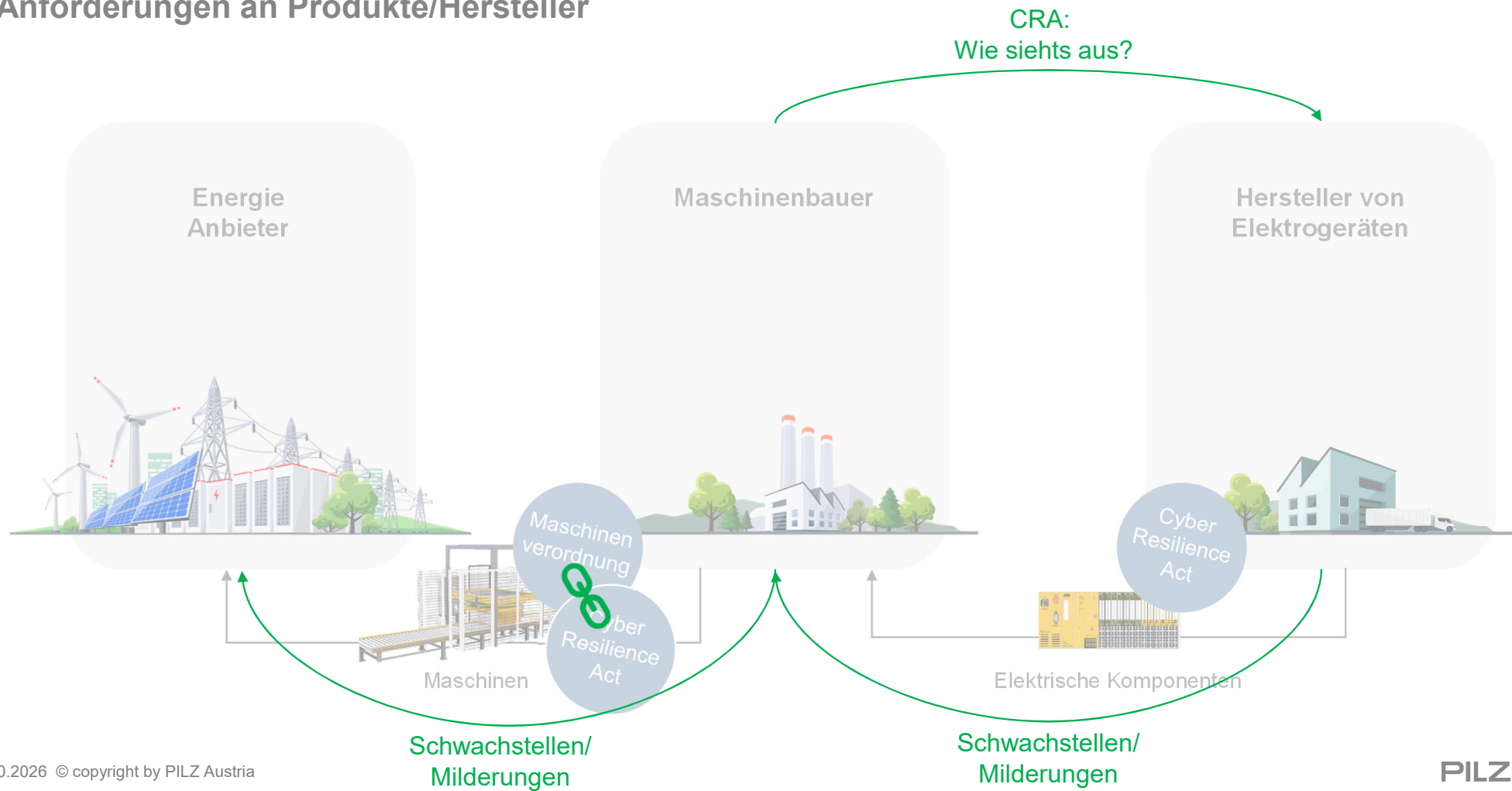
Informieren Sie sich über
Schwachstellen Ihrer Lieferanten



Setzen Sie Prozesse für
MVO&CRA auf

► Zusammenfassung

Anforderungen an Produkte/Hersteller



Fragen oder Anliegen zu **Industrial Security?** Ich freue mich auf Ihre Kontaktaufnahme!



Maximilian Traxler
Innovative Industrial Security für eine
sichere Zukunft

Maximilian Traxler

Pilz Ges.m.b.H., Wagramer Straße 19, 1220 Wien

Tel.: +43 1 7986263 59, Mobil: +43 664 1278552, E-Mail: m.traxler@pilz.at, Internet: www.pilz.at



www.pilz.com



© Pilz GmbH & Co. KG 2025

CECE, CHRE, CMSE®, INDUSTRIAL PI®, Leansafe®, Myzel®, PAS4000®, PASca®, PASconfig®, Pilz®, PIT®, PMCprimo®, PMCprotego®, PMctendo®, PMD®, PMI®, PNOZ®, Primo®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, THE SPIRIT OF SAFETY® sind in einigen Ländern amtlich registrierte und geschützte Marken der Pilz GmbH & Co. KG. Wir weisen darauf hin, dass die Produkteigenschaften je nach Stand und Ausstattungsumfang von den Angaben in diesem Dokument abweichen können. Für die Aktualität, Richtigkeit und Vollständigkeit der in Text und Bild dargestellten Informationen übernehmen wir keine Haftung. Bitte nehmen Sie bei Rückfragen Kontakt zu unserem Technischen Support auf.



PILZ
THE SPIRIT OF SAFETY