VDMA

TECHNICKPOLITIK UND STANDARDISIERUNG

Cyber Resillience Act in a nutshell

Was kommt auf Hersteller zu?

23.09.2025, ALEXEY MARKERT

Wer ist mit dem CRA vertraut?

Agenda

01 HINTERGRUND

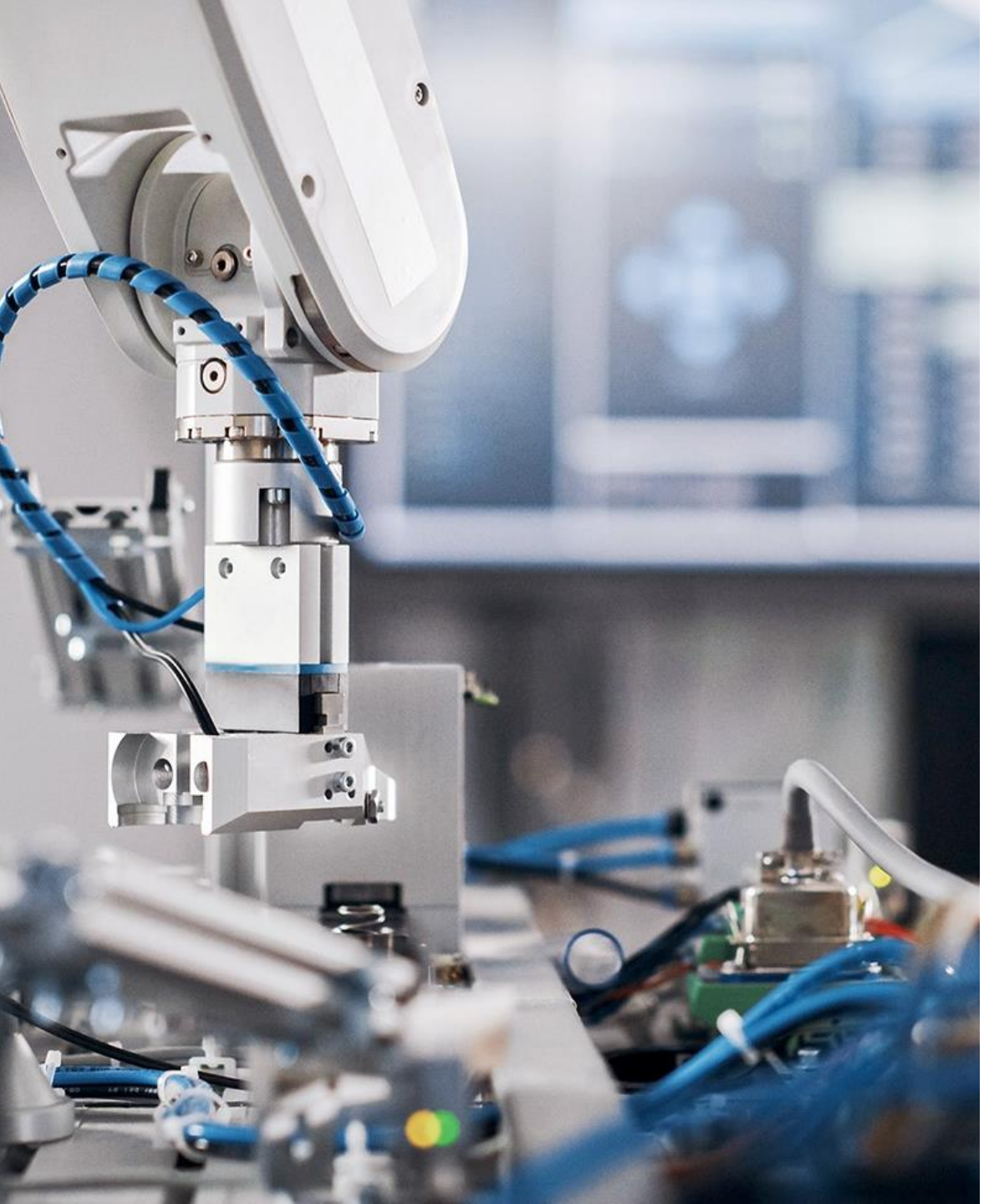
02 ZEITPLAN

03 ANWENDUNGSBEREICH

04 HERSTELLERPFLICHTEN UND ANFORDERUNGEN

05 PRODUKTKATEGORIEN

06 DOWNLOADS UND HILFESTELLUNGEN

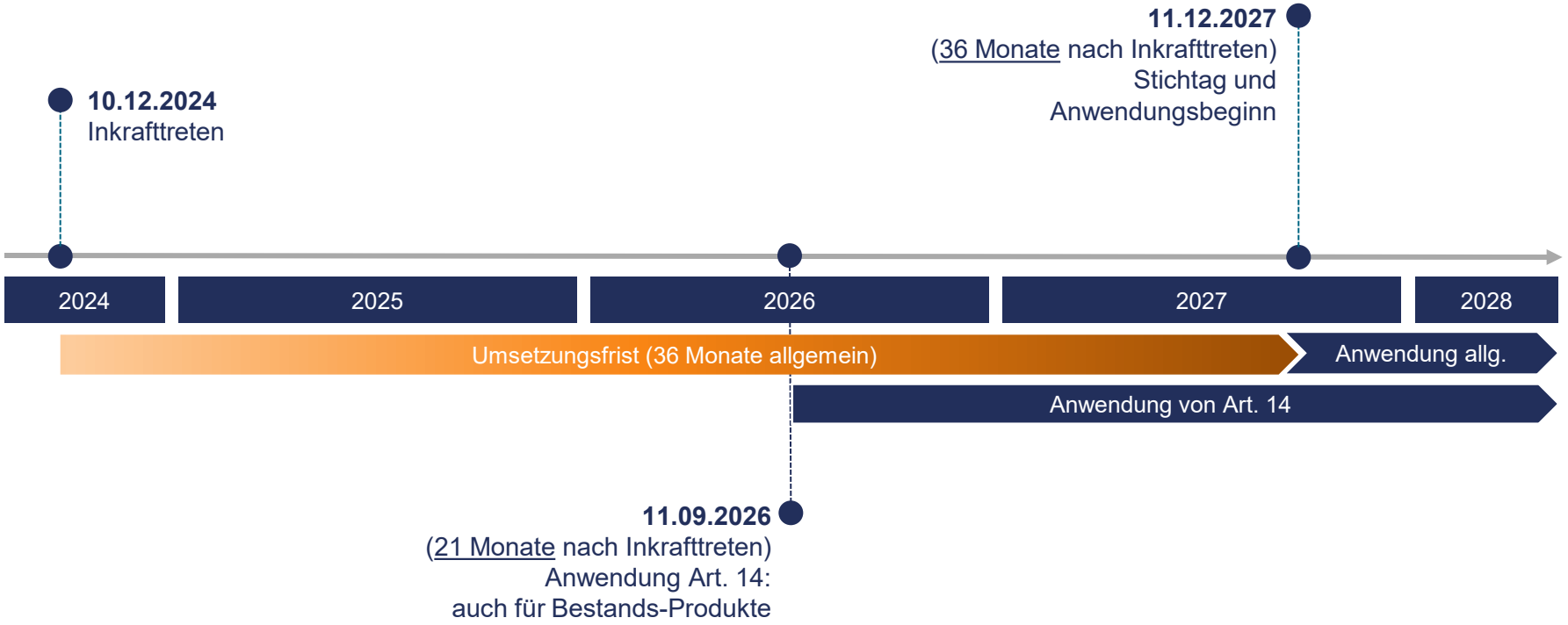


HINTERGRUND

Cyber Resilience Act

- EU-Verordnung
- Im Rahmen des NLF
- Teil der CE-Kennzeichnung
- Etablierung von Rahmenbedingungen für die Cybersicherheit auf Produktebene
- Erfasst werden digitale Produkte einschließlich Soft- und Hardware.

CRA – Finaler Zeitplan



Art. 14 Meldepflichten der Hersteller

Meldung von aktiv ausgenutzten Schwachstellen

Meldung von schwerwiegenden Vorfällen

<u>Meldung an Meldeplattform</u>

nach Kenntnisnahme

Diverse Fristen sind zu wahren

<u>Meldung an Nutzer</u>

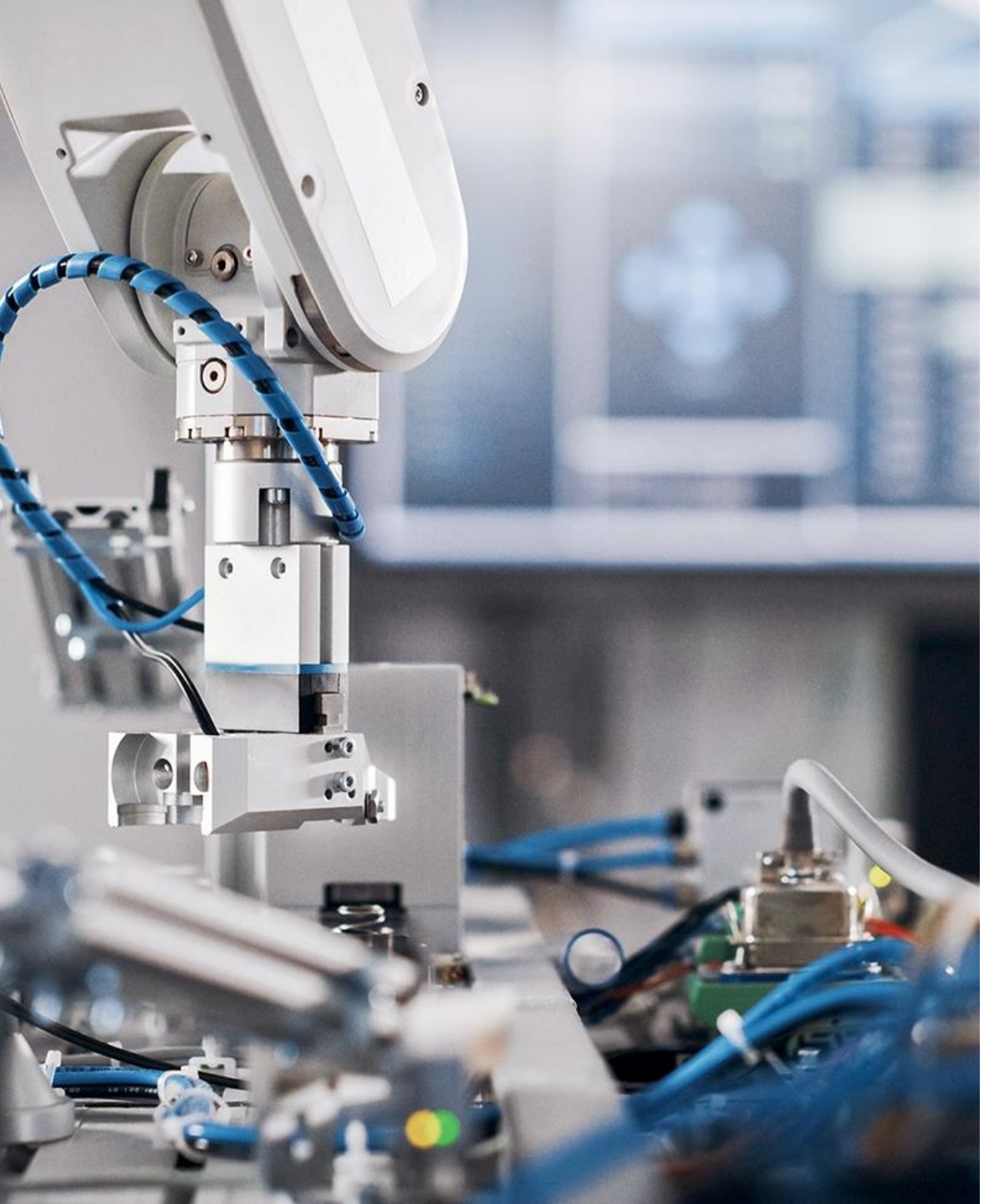
nach Kenntnisnahme

Ohne Frist

Aber:

Reine Meldung

Keine Behebung



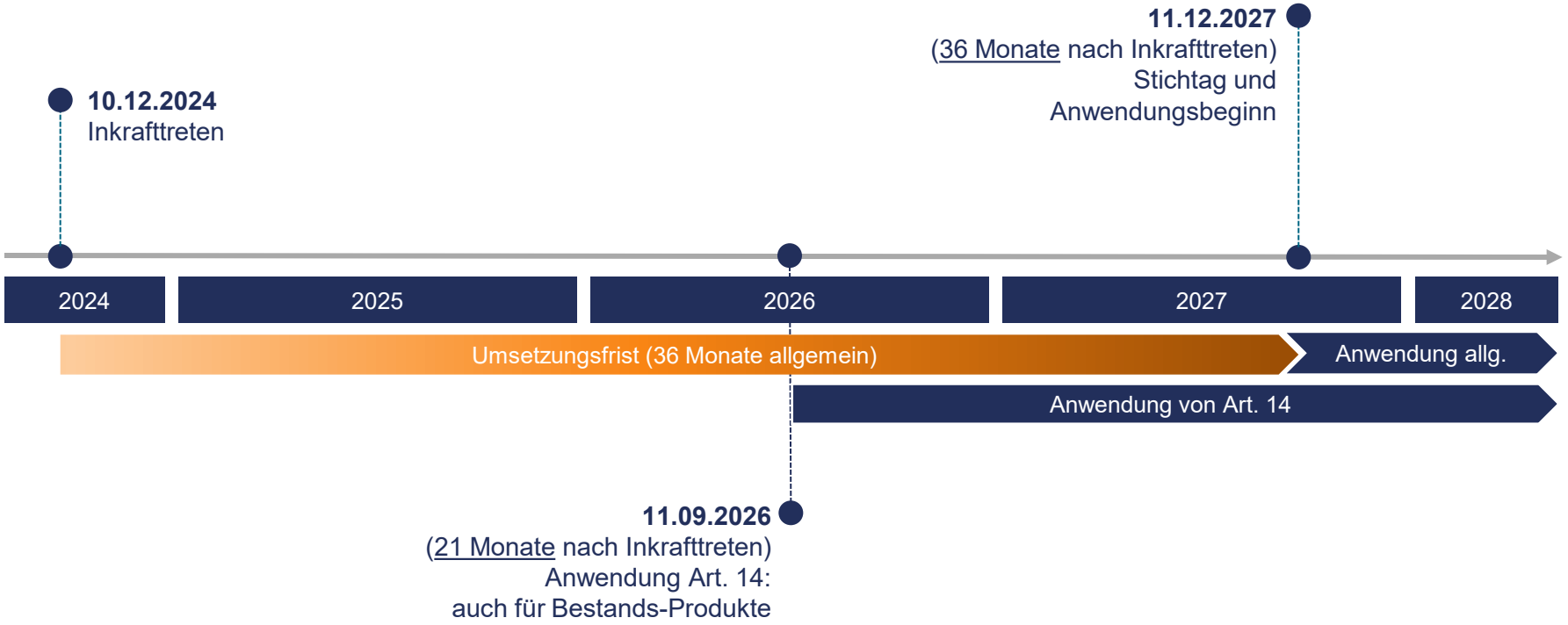
ZEITPLAN

Anwendung von Art. 14 gilt auch für Bestandsprodukte!

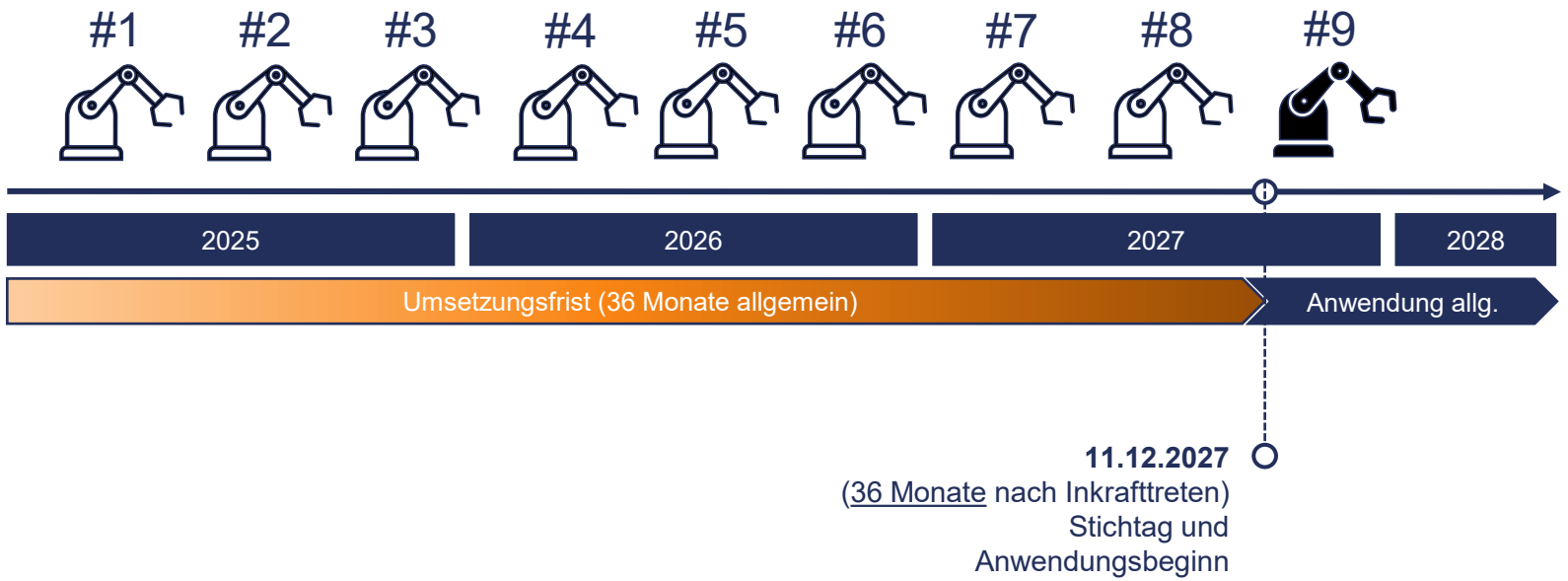
- Art. 69 Abs. 3 “Übergangsbestimmungen”

- *(…) die in Artikel 14 festgelegten Pflichten gelten für alle Produkte, die in den Anwendungsbereich fallen und **vor dem** Anwendungsstichtag in Verkehr gebracht wurden.*

CRA – Finaler Zeitplan

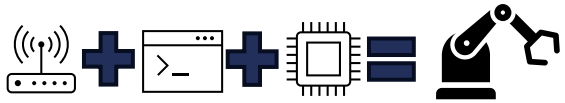


Es gibt keinen Bestandsschutz!



- Neun baugleiche Produkte mit digitalen Elementen
- Neun „Inverkehrbringungen“
- Inverkehrbringung Produkt #9 nach Stichtag
- Produkt #9 muss CRA

Es gibt keinen Bestandsschutz!



- Inverkehrbringung von Komponenten für Produkt #9 vor Stichtag
- Folge: Komponenten fallen nicht unter den CRA
- Produkt #9 muss CRA dennoch erfüllen

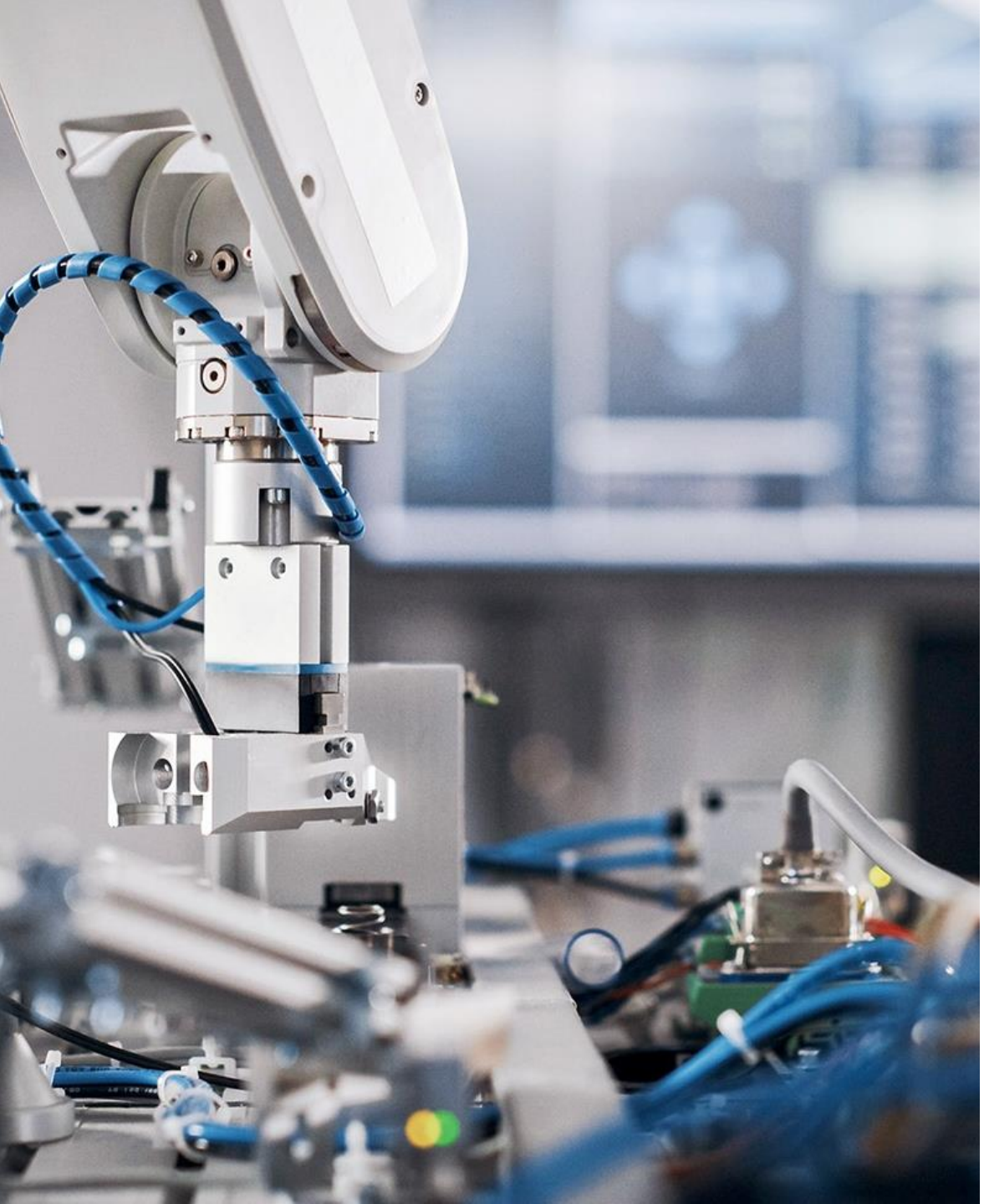
Anwendungsbereich und Begriffsbestimmungen

- Art. 2 (1)
  - Diese Verordnung gilt für (…) Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine **direkte** oder **indirekte logische** oder **physische Datenverbindung** mit einem Gerät oder Netz einschließt.
- Art. 3 (1)
  - „Produkt mit digitalen Elementen“ ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden;

Ausnahmeregelungen

- **Nicht** im Anwendungsbereich:
  - Medizinprodukte (Verordnung EU 2017/745)
  - In-vitro-Diagnostika (Verordnung EU 2017/746)
  - Kraftfahrzeuge (Verordnung EU 2019/2144)
  - Zivilluftfahrt (Verordnung EU 2018/1139)
  - Schiffsausrüstung (Richtlinie 2014/90/EU)
  - Produkte, die ausschließlich für militärische Zwecke konzipiert sind.
  - **Ersatzteile, die identische Bauteile ersetzen, und die nach denselben Spezifikationen hergestellt werden wie die Bauteile, die sie ersetzen sollen.**
  - **Open Source Software**

- **Im** Anwendungsbereich:
  - Bei wesentlichen Veränderungen nach dem Stichtag.
  - **Tailor made products (maßgeschneiderte Produkte)**



Anforderungen an digitale Produkte

Grundlegende Anforderungen nach Annex I Teil

- In Verkehr bringen ohne bekannte ausnutzbare Schwachstellen
- Design mit limitierter Angriffsfläche
- Bereitstellung von kostenlosen Sicherheitsupdates
- uvm.

Schwachstellenmanagement Annex I Teil 2

- Meldung, Behebung und Dokumentation von Schwachstellen
- Erstellung einer SBOM
- Regelmäßige Überprüfungen der Sicherheit
- uvm.

Anzuwenden während des Unterstützungszeitraums

- **Mindestzeitraum von 5 Jahren in Abhängigkeit von Produktlebensdauer**

Produktkategorien im CRA

	Products with digital elements **Art. 3 (1)**	**Important products with digital elements** **Annex III Class 1**	**Important products with digital elements** **Annex III Class 2**	**Critical products with digital elements** **Annex IV**
Mindest-anforderungen Konformitäts-bewertung **(Nachweis Erfüllung Annex I)**	Anwendung von Modul A (Hersteller führt Konformitätsbewertung ohne externe Prüfstelle durch)	Ohne Anwendung harmonisierter Normen: Modul B und C oder Modul H oder EU Cybersicherheits-zertifikat nach VO (EU) 2019/881 Bei Anwendung harmonisierter Normen: Modul A	Anwendung von: Modul B und C oder Modul H oder EU Cybersicherheits-zertifikat nach VO (EU) 2019/881	EU Cybersicherheits-zertifikat nach VO (EU) 2019/881 Keine Voraussetzungen nach Art. 8 (1) erfüllt: Modul B und C oder Modul H
Bestimmungen	Art. 6 Art. 32 (1) Annex VIII Teil 1	Art. 7 Art. 32 (2) Annex VIII Teil 2&3	Art. 7 Art. 32 (3) Annex VIII Teil 2&3	Art. 8 Art. 32 (4) Annex VIII Teil 2&3

Einordnung digitaler Produkte im CRA

Über 90% der Produkte mit digitalen Elementen fallen nicht unter Annex III und IV

- Konformitätsselbsterklärung durch den Hersteller (Modul A; analog zu EU Verordnung Maschinen) ist damit ausreichend.

Artikel 7 (1):

- Produkte mit digitalen Elementen, die die Kernfunktionen einer in Anhang III aufgeführten Produktkategorie aufweisen, gelten als wichtige Produkte mit digitalen Elementen und unterliegen den in Artikel 32 Absätze 2 und 3 genannten Konformitätsbewertungsverfahren. Die Integration eines Produkts mit digitalen Elementen, das die Kernfunktionen einer in Anhang III aufgeführten Produktkategorie aufweist, führt für sich genommen nicht dazu, dass das Produkt, in das es integriert ist, den Konformitätsbewertungsverfahren gemäß Artikel 32 Absätze 2 und 3 unterliegt.

Daraus folgt:

- Einordnung in digitales, wichtiges digitales und kritisches digitales Produkt nach Kernfunktionalität.
- Endprodukt kann wichtige oder kritische Komponenten nach Annex III und IV enthalten ohne dass sich die Anforderungen des Konformitätsbewertungsverfahrens

CRA und die EU-Verordnung Maschinen Annex III 1.1.9

Annex III Nr. 1.1.9 „Schutz gegen Korrumpierung“

- *Die Maschine bzw. das dazugehörige Produkt muss so konstruiert und gebaut sein, dass der Anschluss von einer anderen Einrichtung an die Maschine oder das dazugehörige Produkt durch jede Funktion der angeschlossenen Einrichtung selbst oder über eine mit der Maschine bzw. dem dazugehörigen Produkt kommunizierende entfernte Fernzugriffseinrichtung* ***nicht zu einer gefährlichen Situation führt*** […]

- Die Anforderung betrifft die sicherheitstechnischen Auswirkungen eines Cyberangriffs
- Nicht adressiert werden Resilienz-Anforderungen gegen Cyberangriffe, wie sie der Cyber Resillience Act (CRA) erfasst

Downloads

VDMA FAQ zum CRA Auflage 1.5

Link: VDMA FAQ zum EU Cyber Resilience Act verfügbar - vdma.eu - VDMA

Download CRA EUR-Lex

Link: Regulation - 2024/2847 - EN - EUR-Lex

Jetzt handeln!

KONTAKT

Danke für Ihre Aufmerksamkeit.

FÜR WEITERE INFORMATION MELDEN SIE SICH GERNE BEI:

Alexey Markert

VDMA Technikpolitik und Standardisierung
Lyoner Str. 18
60528 Frankfurt

+49 69 6603-1250
alexey.markert@vdma.eu