

CRA-Einordnung Ihrer Produkte mit digitalen Elementen

Verordnung (EU) 2024/2847 — welches Produkt fällt darunter, in welche Kategorie, mit welcher Folge

BERICHT-NR.	STAND	BEARBEITUNG	UMFANG
CRA-2026-001	25. August 2026	Marta Tsarenko	5 Produkte

Was dieser Bericht ist — und was nicht

Dies ist ein Musterbericht mit erfundenen Produkten. Er zeigt Aufbau, Tiefe und Sprache eines CRA-Checks, damit Sie vor der Beauftragung wissen, was Sie bekommen. Wir ordnen ein und dokumentieren: keine Rechtsberatung, keine Sicherheitsprüfung Ihrer Firmware, keine Konformitätsbewertung. Prüfen und unterschreiben tun Sie.

Übersicht

NR.	PRODUKT	TECHNISCHE AUSSTATTUNG	EINORDNUNG
1	Sensormodul SM-14	4–20 mA Analogausgang · keine Firmware-Schnittstelle · kein Update-Weg	nicht erfasst
2	Steuermodul CM-220	CAN-Bus zur Anlagensteuerung · Firmware-Update über Servicestecker · keine Netzanbindung	erfasst · Standardkategorie
3	Bediengerät HMI-7	eingebettetes Linux · Ethernet · Fernwartung über integrierten VPN-Client	erfasst · Einordnung zu klären
4	Gateway GW-4	koppelt Feldbus auf Ethernet/TCP · kein Internetanschluss · Webserver zur Konfiguration	erfasst · Standardkategorie, mit Vorbehalt
5	Konfigurationssoftware CfgTool 3	Windows-Anwendung · lädt Parameter und Firmware auf CM-220 und GW-4	erfasst · Standardkategorie

Von fünf Produkten fällt eines nicht unter die Verordnung, zwei sind eindeutig der Standardkategorie zuzuordnen, bei zweien hängt die Einordnung an einer Frage, die Sie beantworten müssen — nicht wir. Diese offenen Punkte stehen auf den folgenden Seiten jeweils am Ende der Produktkarte.

Die Produkte im Einzelnen

1 Sensormodul SM-14

NICHT ERFASST

4–20 mA Analogausgang · keine Firmware-Schnittstelle · kein Update-Weg

Fällt nicht in den Anwendungsbereich der Verordnung.

Der CRA gilt nach Artikel 2 Absatz 1 für Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netz einschließt. Ein reiner Analogausgang ist keine Datenverbindung in diesem Sinne.

Fundstelle: Art. 2 Abs. 1 · Art. 3 Nr. 1

OFFENER PUNKT

Sobald eine Variante mit IO-Link, HART oder einem Diagnoseanschluss angeboten wird, kippt die Einordnung. Die Entscheidung gehört deshalb in die Produktakte, nicht nur in eine E-Mail.

2 Steuermodul CM-220

ERFASST · STANDARDKATEGORIE

CAN-Bus zur Anlagensteuerung · Firmware-Update über Servicestecker · keine Netzanbindung

Produkt mit digitalen Elementen, kein wichtiges Produkt nach Anhang III.

Der CAN-Anschluss ist eine physische Datenverbindung, der Anwendungsbereich ist damit eröffnet. Anhang III Klasse I Nummer 14 erfasst „Mikrocontroller mit sicherheitsrelevanten Funktionen“ — der verbaute Controller übernimmt hier keine Sicherheitsfunktion im Sinne der Verordnung, und das Modul als Ganzes entspricht keiner der 19 Kategorien der Klasse I.

Fundstelle: Anhang III Klasse I Nr. 14 (nicht einschlägig) · Anhang I Teil I und II

OFFENER PUNKT

Der Servicestecker ist der kritische Punkt: Ein Update-Weg ohne Signaturprüfung ist mit Anhang I Teil I Nummer 2 Buchstabe b schwer vereinbar. Das ist die erste technische Nachrüstung, die wir empfehlen würden.

3 Bediengerät HMI-7

ERFASST · EINORDNUNG ZU KLÄREN

eingebettetes Linux · Ethernet · Fernwartung über integrierten VPN-Client

Produkt mit digitalen Elementen. Ob wichtiges Produkt der Klasse I, hängt an der Kernfunktion des Geräts.

Zwei Kategorien kommen in Betracht: Anhang III Klasse I Nummer 5 („Produkte mit der Funktion eines virtuellen privaten Netzes“) und Nummer 11 („Betriebssysteme“). Die Durchführungsverordnung (EU) 2025/2392 vom 28. November 2025 stellt klar, dass für die Einordnung die Kernfunktionalität maßgeblich ist — ein Gerät mit eingebautem VPN-Client wird dadurch nicht zum VPN-Produkt, ebenso wenig wie ein Betriebssystem mit Browser zum Browser wird.

Fundstelle: Anhang III Klasse I Nr. 5 und Nr. 11 · DVO (EU) 2025/2392

OFFENER PUNKT

Entscheidend ist, wie Sie das Gerät bewerben. Wird der VPN-Zugang als Produktmerkmal vermarktet, spricht viel für Klasse I — und damit für ein anderes Konformitätsbewertungsverfahren nach Artikel 32 Absatz 2. Wird er nur intern für die Fernwartung genutzt, bleibt es bei der Standardkategorie. Diese Frage sollte vor der Katalogtexterstellung entschieden werden, nicht danach.

4 Gateway GW-4

ERFASST · STANDARDKATEGORIE, MIT VORBEHALT

koppelt Feldbus auf Ethernet/TCP · kein Internetanschluss · Webserver zur Konfiguration

Produkt mit digitalen Elementen; nach heutigem Stand kein wichtiges Produkt.

Anhang III Klasse I Nummer 12 nennt „Router, Modems für die Internetanbindung und Switches“. Ein Protokollumsetzer ohne Internetanbindung fällt nach dem Wortlaut nicht darunter; Nummer 6 („Netzmanagementsysteme“) trifft ebenfalls nicht zu.

Fundstelle: Anhang III Klasse I Nr. 6 und Nr. 12 · DVO (EU) 2025/2392

OFFENER PUNKT

Der eingebaute Webserver ist die eigentliche Baustelle — Standardpasswort, offene Ports und ein Update-Weg ohne Rückfallebene sind die drei Befunde, die wir bei Geräten dieser Bauart regelmäßig sehen. Die technischen Beschreibungen der Durchführungsverordnung sollten vor Abschluss der technischen Dokumentation gegengelesen werden.

5 Konfigurationssoftware CfgTool 3

ERFASST · STANDARDKATEGORIE

Windows-Anwendung · lädt Parameter und Firmware auf CM-220 und GW-4

Eigenständige Software ist ein eigenes Produkt mit digitalen Elementen.

Der CRA erfasst Software auch dann, wenn sie getrennt in Verkehr gebracht wird. Für das Werkzeug gelten deshalb eigene Pflichten — eigene technische Dokumentation, eigener Unterstützungszeitraum, eigene Schwachstellenbehandlung.

Fundstelle: Art. 3 Nr. 1 · Anhang I Teil II · Anhang VII

OFFENER PUNKT

In der Praxis wird das Konfigurationswerkzeug fast immer vergessen, weil es „nur ein Tool“ ist. Es ist aber der Weg, auf dem Firmware in Ihre Geräte gelangt — und damit der interessanteste Angriffspfad im ganzen Produktprogramm.

Fristen

TERMIN	WAS GILT	WAS DARAUS FOLGT
11. September 2026	Meldepflichten nach Artikel 14 gelten	Aktiv ausgenutzte Schwachstelle: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht spätestens 14 Tage, nachdem eine Korrektur bereitsteht. Schwerwiegender Sicherheitsvorfall: 24 Stunden, 72 Stunden, Abschlussbericht binnen eines Monats. Adressat ist das koordinierende CSIRT und parallel die ENISA über die einheitliche Meldeplattform.
11. Dezember 2027	Verordnung in voller Anwendung	Sicherheitsanforderungen nach Anhang I Teil I, Schwachstellenbehandlung nach Anhang I Teil II, Nutzerinformationen nach Anhang II, technische Dokumentation nach Anhang VII, Konformitätsbewertung und CE-Kennzeichnung.
Unterstützungszeitraum	Artikel 13 Absatz 8	In der Regel mindestens fünf Jahre; kürzer nur, wenn das Produkt erwartbar kürzer im Betrieb ist. Für Industrieprodukte mit langer Nutzungsdauer ist ein längerer Zeitraum zu begründen — und er ist vor dem Inverkehrbringen festzulegen, nicht danach.

Nächste Schritte

1. Die beiden offenen Einordnungsfragen entscheiden (HMI-7: Wird der VPN-Zugang vermarktet? GW-4: technische Beschreibungen der Durchführungsverordnung gegenlesen).
2. Bis zum 11. September 2026 einen Meldeweg festlegen: Wer bemerkt eine ausgenutzte Schwachstelle, wer meldet, an wen, mit welchem Text. Eine Seite genügt — aber sie muss vorher existieren.
3. Für jedes erfasste Produkt den Unterstützungszeitraum festlegen und begründen.
4. Technische Dokumentation nach Anhang VII aufsetzen — parallel zur Maschinenverordnung, nicht danach, denn beide greifen auf dieselben Konstruktionsunterlagen zu.