Die Bahnindustrie.
Verband der Bahnindustrie in Deutschland

Leitfaden

CRA-Leitfaden

Gesetz über horizontale Cybersicherheits-anforderungen für Produkte mit digitalen Elementen

Inhalt

1 Allgemeines

1.1 Präambel

Die Inhalte von ➔ Kapitel 2 dieses Leitfadens wurden auf Grundlage der „Expert Guidance on the Implementation of the Cyber Resilience Act in Mainline and Urban Railways“ mit freundlicher Genehmigung der Cybersecurity Rail Sector Group erarbeitet.[1]

1.2 Einführung

Der europäische Cyber Resilience Act (CRA) ist die erste und weltweit einmalige Verordnung, die ein Mindestmaß an Cybersicherheit für sogenannte „Produkte mit digitalen Elementen“ (PDE) festlegt, die ab dem 11.12.2027 auf dem EU-Markt in Verkehr gebracht werden. PDE umfassen dabei sowohl vernetzte Hardware- als auch Software-Produkte, mit logischen oder physischen Schnittstellen zur Datenverbindung.

Der Schienenverkehr zeichnet sich durch die lange Lebensdauer und langen Entwicklungszyklen seiner Produkte aus. Aus diesem Grund ist es herausfordernd, Fortschritte im Bereich der Cybersicherheit im Schienenverkehr so umzusetzen, dass der laufende Betrieb und die Entwicklung des Eisenbahnsystems und seiner Projekte aufrechterhalten bleiben.

Der Leitfaden unterstützt die Hersteller (und alle weiteren Wirtschaftsakteure im Sinne des CRA) dabei, die Anforderungen des CRA ordnungsgemäß zu erfüllen – und trägt damit zugleich dazu bei, mögliche Sanktionen aufgrund von Nichtkonformität zu vermeiden. Nichtkonformität kann zu erheblichen Sanktionen führen: gemäß ↗ CRA Artikel 64 maximal zu 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes als Schadenersatz, je nachdem, welcher Betrag höher ist. Die Strafen können je Produkt erhoben werden und stellen damit ein noch deutlich höheres Unternehmensrisiko dar, wenn grundsätzlich gegen die Anforderungen verstoßen wird. Darüber hinaus kann die Marktbehörde eine verbindliche Aufforderung zum Rückruf aller betroffenen vertriebenen PDEs verlangen ↗ CRA Artikel 13 (21).

Der VDB und seine Mitglieder – die Hersteller und Integratoren für den deutschen und europäischen Bahnsektor – unterstützen die Ziele des CRA uneingeschränkt und setzen sich für deren schnellstmögliche Umsetzung ein. Dieser Leitfaden zeigt, dass der CRA-Text bereits Instrumente für eine reibungslose und ordnungsgemäße Umsetzung bereitstellt und dass sein risikobasierter Ansatz dazu beitragen kann, schwerwiegende Störungen in der Lieferkette des Eisenbahnsektors und im gesamten Sektor zu verhindern.

Aufgrund seines horizontalen, sektorübergreifenden Charakters enthält der CRA-Text jedoch keine vorgefertigten sektorspezifischen oder operativen Leitlinien für die Anwendung seiner Flexibilitäten, wie z. B. Präzisierungen zu Formulierungen wie „soweit technisch möglich“ und

1 Cybersecurity Rail Sector Group, bestehend aus UNIFE, EIM, CER, EUG, UITP Europe.

„soweit anwendbar“. Darüber hinaus verwendet der CRA Begriffe und Konzepte, die in der bahnspezifischen Gesetzgebung nicht vorkommen, obwohl sie sich teilweise mit dieser überschneiden. Für den Eisenbahnsektor, der durch komplexe Systeme, Teilsysteme und Komponenten innerhalb einer Lieferkette mit zahlreichen Beteiligten gekennzeichnet ist, können Ungenauigkeiten zu Missverständnissen oder unterschiedlichen Auslegungen zwischen den Beteiligten oder sogar zwischen Projekten führen. Das könnte potenzielle Verkehrs-, Funktions- oder Betriebsstörungen zur Folge haben.

Um dies zu vermeiden, enthält der vorliegende technische Leitfaden, der im Zeitraum von April 2025 bis Februar 2026 vom Arbeitsausschuss Cyber- und Informationssicherheit (CIS) des VDB entwickelt wurde, **operative unverbindliche Empfehlungen** für den Sektor und die Beteiligten in Form von Kriterien und Grundsätzen, die den im Eisenbahnbereich verwendeten risikobasierten Ansatz anwenden. Soweit möglich, wurden die üblichen Praktiken des Eisenbahnsektors auf die Cybersicherheit ausgeweitet. Insbesondere ist es im Eisenbahnbereich häufig der Fall, dass Hersteller Anwendungsbedingungen (z. B. Safety-Related Application Conditions -SRACs) an ihre Nutzer weitergeben. Dieses Konzept wurde bereits in der TS 50701 für die Cybersicherheit angepasst und wird hier zur Anwendung gebracht. Voraussetzung ist die gegenseitige Akzeptanz dieser Anwendungsbedingungen, ohne daraus eine Verschiebung der Verantwortung im Sinne des CRA zu erwirken. Mit diesem pragmatischen Ansatz will der Sektor detailliert operative unverbindliche Empfehlungen, **wie die CRA-Konformität für Eisenbahnkomponenten und -systeme nachgewiesen werden kann** und wie die verfügbaren Flexibilitäten am besten genutzt werden können, um die CRA-Anforderungen effektiv zu erfüllen. Durch diesen Ansatz soll der Leitfaden eine pragmatische und konsistente Verbesserung der Cybersicherheit für den Sektor ermöglichen, wodurch Unsicherheiten und Lähmungen bei den Umsetzungsbemühungen vermieden werden.

1.3 Geltungsbereich und Abgrenzungen

Dieser Leitfaden enthält Erläuterungen und branchenweite unverbindliche Empfehlungen für die Umsetzung der ↗ Verordnung (EU) 2024/2847 – dem Gesetz über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen – kurz CRA – und ihrer Verpflichtungen mit dem Ziel, dem Eisenbahnsektor bei der schnellen und wirksamen Umsetzung der Verordnung zu dienen. Der Leitfaden erläutert die bestehende Verordnung und soll deren Verständnis und die Wirksamkeit ihrer Umsetzung unterstützen. Es handelt sich bei diesem Dokument nicht um eine rechtliche Beratung durch den VDB oder die Untergruppe CIS. Vielmehr ist jedes vom CRA betroffene Unternehmen selbst für die Umsetzung des CRA verantwortlich. Das Dokument beinhaltet ebenfalls keinerlei verpflichtende Regelungen, sondern allgemeine unverbindliche Empfehlungen, es kann weder gegenüber Vertragspartnern noch gegenüber Behörden als Rechtfertigung für eine CRA Umsetzung genutzt werden.

Die CRA-Konformitätserklärung ist eine Aufgabe des Herstellers und in seiner Verantwortung. Sie dient nicht dazu, nutzerspezifische Anforderungen hinsichtlich eines spezifischen Security-Niveaus zu erfüllen.

1.4 Abkürzungen

Abkürzung	Bedeutung
ADCO	Besondere Gruppe zur administrativen Zusammenarbeit (CRA Artikel 52.15)
ASIC	Application Specific Integrated Circuit; Prozessor der für spezielle Aufgaben konstruiert wurde, z. B. in Switchen zu finden
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTM	Balise-Transmission-Module
CBTC	Communication-Based Train Control
CCTV	Closed Circuit Television; Videoüberwachungssystem
CER	Communauté européenne du rail/Europäische Interessensvertretung der Bahnbetreiber
CIS	Arbeitsausschuss Cyber- und Informationssicherheit
COTS	„components-off-the-shelf“ oder „commercial off-the-shelf“
CPU	Central Processing Unit
CRA	Gesetz über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen – kurz CRA; EU Verordnung (EU) 2024/2847
CSIRT	Computer Security Incident Response Team
CSRG	Cybersecurity Rail Sector Group
CVE	Common vulnerabilities and exposures
DMI	Driver Machine Interface
DiPro_x	Digital Produkt; imaginärer Name für ein Produkt mit digitalen Elementen
DMZ	Demilitarisierte Zone; Bereich zwischen Netzwerken, in dem gemeinsam genutzte Inhalte gehostet werden.
EDR	Endpoint Detection and Response
EIM	European Rail Infrastructure Managers; Interessenvertretung der Bahninfrastrukturbetreiber
ENISA	European Union Agency for Cybersecurity
ERJU	Europe‘s Rail Joint Undertaking
ETCS	European Train Control System
EIU	Eisenbahninfrastrukturunternehmen
EUG	ERTMS Users Group ertms.be/activities/ertms-security-core-group
EUVD	EU Vulnerability Database
EVC	European Vital Computer
EVU	Eisenbahn Verkehrsunternehmen
FPGA	Field Programmable Field Array; Einheit in der Logikgatter per Software verknüpft werden können

Abkürzung	Bedeutung
FRMCS	Future Railway Communication System
GL	Guideline (Leitfaden)
GSM	Global System for Mobile Communications; Mobilfunknetz der zweiten Generation
HMI	Human Machine Interface
HSM	Hardware-Sicherheitsmodul
HVAC	Klimaanlage
IAM	Identity and Access Management
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission; Standard-Prefix für internationale Standards, die durch die IEC veröffentlicht wurden, z. B. IEC 62443
IPS	Intrusion Prevention System
KMC	Key Management Centre
NIS-2	Richtlinie des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, Richtlinie (EU) 2022/2555
NIS2UmsG	Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung; Deutsche, nationale Umsetzung des NIS-2 vom 05.12.2025, in Kraft zum 06.12.2025
OJEU	Official Journal of the European Union; Amtsblatt der Europäischen Union
PDE	Produkt mit Digitalen Elementen
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
RBC	Radio Block Centre
SBOM	Software Bill of Material
SCADA	Supervisory Control and Data Acquisition
SecRAC	Security-Related Application Conditions
SL	Security Level nach IEC 62443-3-3 und -4-2.
SN	Seriennummer
SRAC	Safety Related Application Conditions
SIEM	Security Information and Event Management; System zur Sammlung und Auswertung von securityrelevanten Logdaten
SPS	Speicherprogrammierbare Steuerung
TCMS	Train Control Management System
TPM	Trusted Platform Module; Chip auf Mainboards zum Schutz vor illegitimen Betriebssystemen

Abkürzung	Bedeutung
TS	Technical Standard (Technischer Standard), z. B. TS 50701 für Cybersecurity im Bahn-Sektor
TSI	Technische Spezifikationen für die Interoperabilität
UNIFE	Union des Industries Ferroviaires Européennes/Verband der europäischen Bahnindustrie
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
XDR	Extended Detection and Response:Einheitliche Plattform zur Erkennung und Reaktion auf Sicherheitsvorfälle, die KI und Automatisierung nutzt
ZCR	Zonen- und Conduitanforderungen (en: Zone and conduit requirement); wird in der IEC 62443-3-2 verwendet, um die Prozessschritte für das Risikomanagement zu bezeichnen.

Tabelle 1: Abkürzungen

1.5 Begriffsdefinitionen

Zur Vereinfachung der Lesbarkeit sind in diesem Dokument Definitionen, Beispiele und Hinweise optisch hervorgehoben.

DEFINITIONEN Quellen, sofern nicht an den jeweiligen Textstellen gesondert angegeben, sind die Cyberresilienz-Verordnung 2024/2847 der Europäischen Union (CRA) oder der Leitfaden „Blue Guide“ für die Umsetzung der Produktvorschriften der EU 2022.

BEISPIELE dienen der Veranschaulichung und Praxisanwendung regulatorischer Anforderungen im Bahnkontext.

HINWEISE ergänzen Definitionen und Beispiele um Klarstellungen und Auslegungshinweise, insbesondere zur Vermeidung von Fehlinterpretationen.

Grundlegende Begriffe im Dokument

Begriff	Verwendung
Auswirkungen	Potenzielle Auswirkungen von erfolgreichen Angriffen, in Auswirkungskategorien (z. B. „Gering“, „Mittel“, „Hoch“) bewertet und nach Schutzzielen differenziert.
Eintrittswahrscheinlichkeit (Likelihood)	Wahrscheinlichkeit (qualitativ, nicht quantitativ), dass ein Angreifer eine Sicherheitslücke erfolgreich ausnutzt und eine Bedrohung initiiert, von der ein Risiko ausgeht.
Sicherheitslücke	Abweichung des PDE oder dessen Betriebsumgebung vom „Best Practice“

Begriff	Verwendung
Schwachstelle	Sicherheitslücke in Software, die bei einer Cyberbedrohung ausgenutzt werden kann. Sie ist regelmäßig als „Vulnerability“ mit „CVE-ID“ in internationalen Datenbanken identifiziert.
Security/Sicherheit	In diesem Dokument repräsentiert das Wort „Security“ die Begriffe „Cybersecurity“ und „IT-/OT-Sicherheit“. Wenn in diesem vorliegenden Leitfaden von „Sicherheit“ gesprochen wird, soll hiermit klargestellt sein, dass es sich stets um die Security handelt und die im Bahnbereich vertretene Funktionale Sicherheit (Safety) ausgeschlossen ist.

Tabelle 2: Grundlegende Begriffe

2 Grundsätzliches zum CRA

2.1 Zeitplan für die Anwendung

Der CRA gibt den folgenden Zeitplan vor:

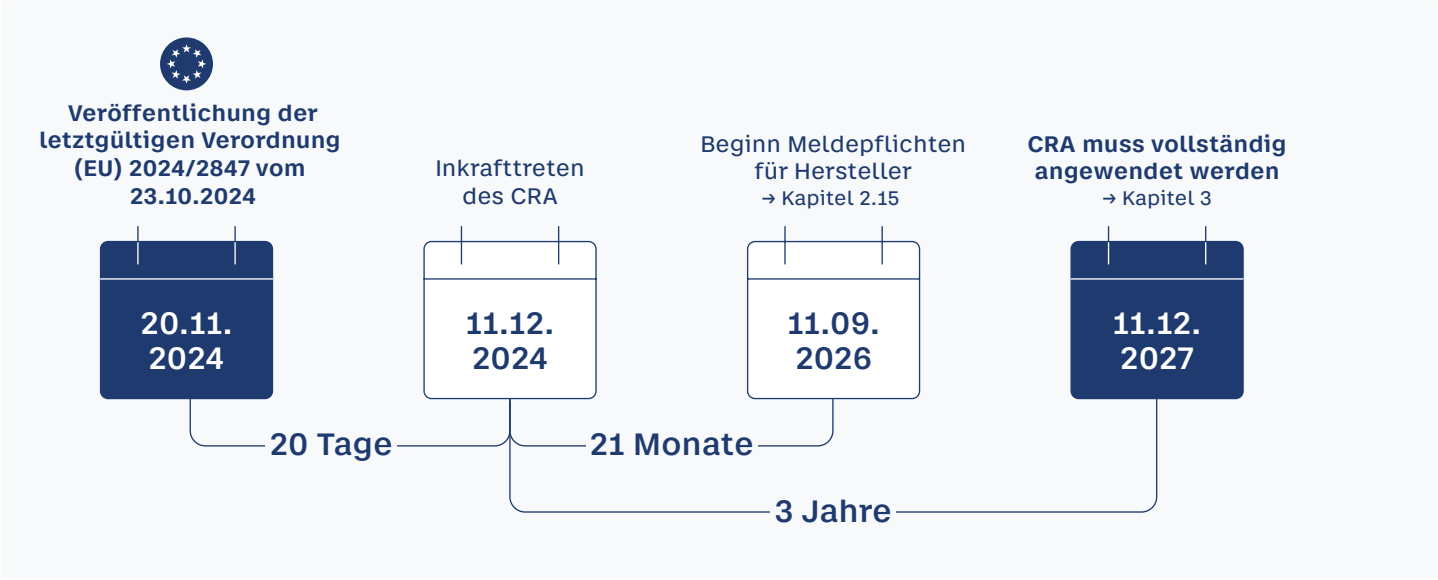

Abbildung 1: Zeitplan CRA

Aktuelle Informationen über die im Zusammenhang mit dem CRA noch in Kraft zu setzenden Rechtsakte sind auf dieser Webpage der Europäischen Kommission[2] verfügbar.

2.2 Rollendefinition

Gemäß CRA muss die Security über die gesamte Lieferkette mit unterschiedlichen Pflichten in verschiedene Rollen gewährleistet werden.

In der → Tabelle 3 werden die typischen Rollen innerhalb der Bahnindustrie den CRA-Rollen zugeordnet. Hierbei können auch mehrere Rollen gleichzeitig eingenommen werden.

		CRA-Rollen			
		Hersteller	**Händler**	**Einführer**	**Nutzer**
Rollen innerhalb der Bahnindustrie	Hersteller	Rollen stimmen hier überein	–	–	Kann Nutzer sein*
	Integrator	Bei Integration von PDE zu einem neuen, integriertem PDE	Bei Verkauf von zugekauften PDE ohne Veränderung	Bei Import und direktem Weiterverkauf	Kann Nutzer sein*
	Eigentümer	Bei eigenständigen Änderungen am PDE	Bei Vermietung oder anderweitiger Überlassung	Bei Vermietung oder anderweitiger Überlassung	Kann Nutzer sein*
	Betreiber	Bei Änderungen am PDE und erneuter Bereitstellung auf dem Markt	–	–	Betreiber ist Nutzer im Sinne des CRA

* In dieser Guideline nicht weiter betrachtet.

Tabelle 3: Rollendefinition

In den nachfolgenden Unterkapiteln werden die Verantwortungen der einzelnen Rollen innerhalb der Bahnindustrie zur Einhaltung des CRAs dargestellt.

2.2.1 Nutzer und Kunde

Entsprechend der Beziehungen innerhalb der Lieferkette sind Kunden beispielsweise:

- Hersteller von Systemen/Teilsystemen/Komponenten – sie erhalten bspw. Security Updates für Steuerungen
- Integratoren – sie erhalten bspw. Installationsanweisungen, Security Updates
- Inbetriebsetzer – sie erhalten bspw. Anweisungen zur In- und Außerbetriebnahme,
- Betreiber – sie erhalten bspw. Betriebsanleitungen und Nutzerhandbücher, Security Updates
- Wartung – sie erhält bspw. Wartungshandbücher und Anweisungen.

All diese Kunden sind im Sinne des CRAs Nutzer. Das heißt, sie erhalten die Informationen, Security Updates etc. entsprechend CRA. **Im Verlauf des Dokuments wird immer vom Nutzer gesprochen.**

In der folgenden ➔ Abbildung 2 wird verdeutlicht, dass jede Rolle in der Lieferkette CRA-Nutzer ist. Das heißt, jeder Integrator, der nicht der ursprüngliche Hersteller eines integrierten PDEs ist, ist ebenfalls ein Nutzer im Sinne des CRAs. Das heißt, er hat auch alle Ansprüche aus dem CRA.

Trotzdem ist es in der praktischen vertraglichen Implementierung möglich, dass ein Nutzer (z. B. Betreiber) einen Wartungsvertrag mit dem Hersteller des Teilsystems (Integrator I)

geschlossen hat, um sicherzustellen, dass der Integrator I regelmäßig Updates liefert und ggf. auch die Wartung übernimmt. In dem Fall, liefert der Integrator II ggf. Updates für nur einen Teil des Produkts, das er dem Nutzer (z. B. Betreiber) liefert. In jedem Fall bleibt aber nach CRA der Anspruch auf die Security Updates bestehen.

Der Vollständigkeit halber ist die Information des Nutzers über detektierte Security-Vorfälle dargestellt (violett). Diese erwächst jedoch aus NIS-2. Der Nutzer hat keine Verpflichtung aus dem CRA heraus.

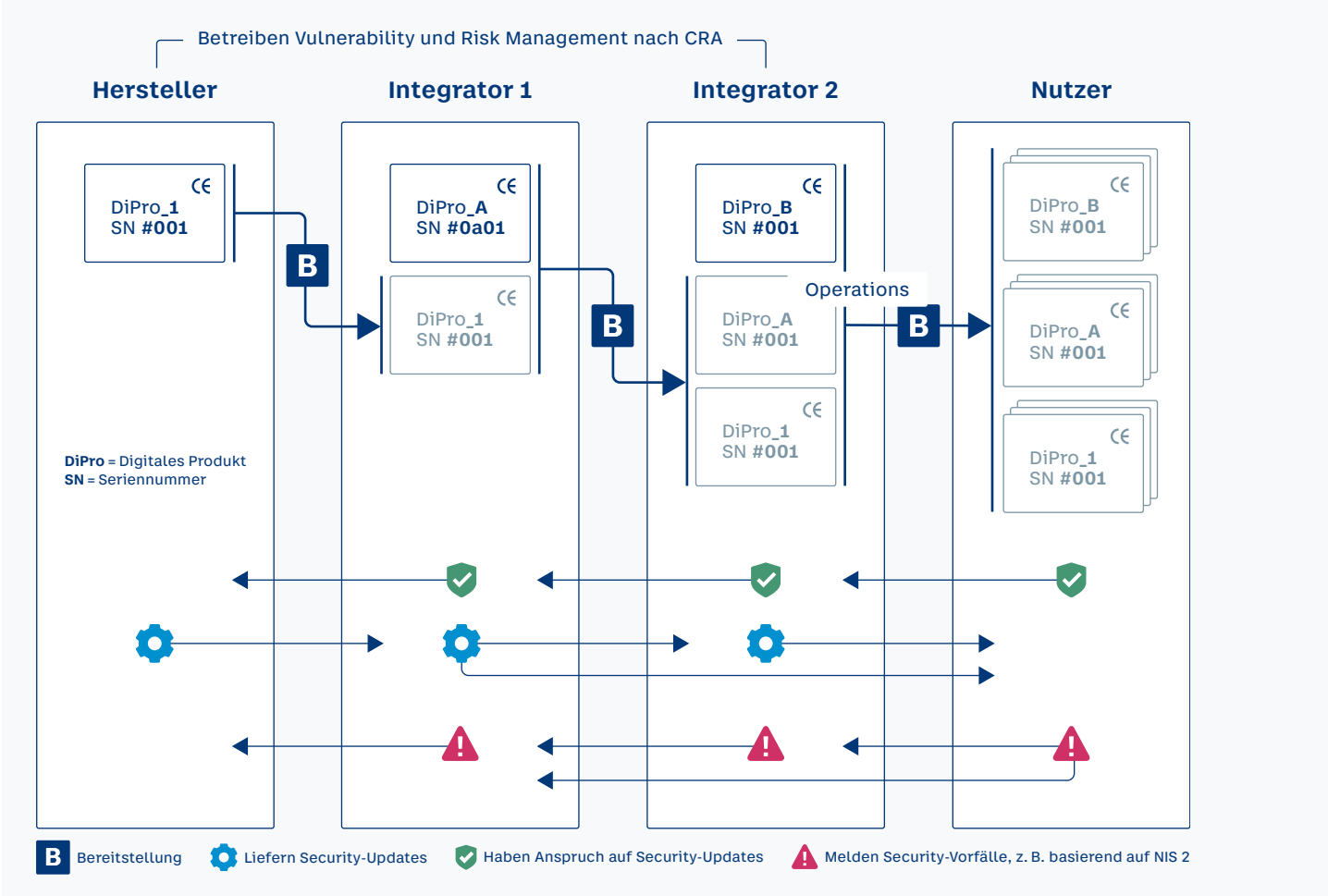

Abbildung 2: Hersteller-Nutzer-Beziehung

2.2.2 Hersteller

Entsprechend der ➔ Tabelle 3 können alle Rollen innerhalb der Bahnindustrie die Rolle des Herstellers von PDEs einnehmen. Die Rolle des Herstellers ist in ↗ CRA Artikel 3 (13) wie folgt definiert:

DEFINITION

Hersteller ist eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich.

Anders formuliert: Ein Hersteller ist jemand, der PDEs selbst produziert, produzieren lässt oder sie einkauft und modifiziert und als eigenes PDE weiterverkauft. Es ist dabei unerheblich, ob es sich um eine Person oder ein Unternehmen handelt. Im Kontext des CRAs werden der Rolle des Herstellers eines PDEs die meisten Verpflichtungen auferlegt:

- Umsetzung der definierten Security-Anforderungen im Systemdesign („Secure by Design“).
- Durchführung von Analysen der Cybersicherheitsrisiken (Risikoanalysen) für das PDE unter Berücksichtigung des Input des Nutzers bzw. Herstellern entlang der Lieferkette.
- Verantwortung bzw. Unterstützung für die CRA-sichere Integration bzw. Entwicklung (Secure Development) und Lieferung von PDEs mit integrierten Security Funktionen (z. B. gemäß IEC 62443).
- Durchführung von Security Nachweisen (z. B. gemäß IEC 62443 oder CENELEC-Normen).
- Bereitstellung von Security Dokumentation entsprechend ↗ CRA Anhang II.
- Verantwortung für die CRA-Konformitätsbewertung für das PDE.
- Verantwortung für Schwachstellen Management entsprechend dem definierten Unterstützungszeitraum für das PDE (z. B. Security Updates, End-of-Life-Kommunikation).

2.2.3 Händler und Einführer

Zum besseren Verständnis der nachfolgenden Kapitel sind hier Rollen des Händlers und des Einführers beschrieben.

Laut Definition ↗ CRA Artikel 3 (17) wird ein Händler wie folgt definiert:

DEFINITION

Händler ist eine natürliche oder juristische Person in der Lieferkette, die ein Produkt mit digitalen Elementen ohne Änderung seiner Eigenschaften auf dem Unionsmarkt bereitstellt, mit Ausnahme des Herstellers oder des Einführers.

Laut Definition ↗ CRA Artikel 3 (16) wird ein Einführer wie folgt definiert:

DEFINITION

Einführer ist eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein Produkt mit digitalen Elementen unter dem Namen oder der Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person in der Union in Verkehr bringt.

Einführern und Händlern werden mehrere Pflichten gegenüber den PDEs auferlegt, die sie **auf dem Markt bereitst**ellen ↗ CRA Artikel 19 und Artikel 20. Sie gelten dann gemäß ↗ CRA Artikel 21 als Hersteller und unterliegen den ↗ CRA Artikel 13 und 14, wenn **sie:**

- ein PDE **unter ihrem Namen oder Marke** auf den Markt bringen oder
- ein PDE **wesentlich verändern** und dieses PDE auf dem Markt bereitstellen.

2.2.4 Integrator

Die Rolle des Integrators ist im CRA nicht definiert, sondern lediglich im ↗ CRA Anhang II (8f) erwähnt. Da der Integrator eine häufig auftretende Rolle im Bahn-Sektor ist, wird hier tiefer auf die Aufgaben – in Abhängigkeit der Art der Integration – eingegangen.

DEFINITION

Die Integration eines PDEs zu einem neuen digitalen Produkt ergibt erneut ein PDE. Für den Integrator ergeben sich daher die gleichen Pflichten wie beim Hersteller. Darüber hinaus kann der Integrator weitere Rollen einnehmen, welche nachfolgend erläutert werden.

2.2.4.1 Integration eigener Produkte

Integriert ein Integrator PDEs aus eigener Herstellung in ein System, das selbst als PDE angesehen wird oder ein neues PDE, so ist er für diese PDE im Sinne des CRA als **Hersteller** zu betrachten, – sofern das betreffende Produkt auf dem Markt bereitgestellt wird. Ihm obliegt damit für die selbst hergestellten PDE die Verpflichtungen des CRA einzuhalten.

2.2.4.2 Integration gekaufter Produkte

Integriert ein Integrator PDEs, die bereits in der EU auf den Markt gebracht wurden in ein System, das selbst ein PDE ist oder ein neues PDE, das er auf dem Markt anbietet, so ist er laut CRA für diese Produkte als **Hersteller** zu sehen.

2.2.4.3 Integration importierter Produkte

Integriert ein Integrator PDE, die aus dem Nicht-EU-Ausland bezogen wurden und durch den Integrator bereitgestellt werden, so nimmt er die CRA-Rolle des **Einführers und Herstellers** ein. Bringt der Integrator das eingeführte PDE nicht allein auf den EU-Markt, sondern nur in integrierter Form, so muss er auf Ebene des integrierten PDE die CRA-Anforderungen sicherstellen. Um dies erfüllen zu können, sollte er sinngemäß ↗ CRA Artikel 19 befolgen. Dies spiegelt auch die wesentlichen Aktivitäten aus ↗ CRA Artikel 13 (5) wider. Bringt der Integrator das Produkt allein auf den Markt, agiert er ausschließlich als Einführer und muss ↗ CRA Artikel 19 befolgen. Dies gilt auch, wenn dieser Vorgang innerhalb einer Unternehmensgruppe – z. B. innerhalb der Digitalprodukt Holding liefert Digitalprodukt Limited Şirket (Türkei) and Digital GmbH (Deutschland) – ausgeführt wird.

2.2.4.4 Integration beigestellter Produkte

Wenn der Integrator ein fertiges Produkt mit digitalen Elementen vom Nutzer (z. B. Betreiber) als unentgeltliche Beistellung zur Verfügung gestellt bekommt und dieses unverändert integriert, gilt: **Keine Herstellerpflichten aus dem CRA**, solange:

- das beigestellte Produkt bereits konform ist (CE-Kennzeichnung, Konformitätserklärung vorhanden)
- der Integrator keine Änderungen vornimmt, die die Security Merkmale beeinflussen.

Wenn die Integration die Security Funktionen beeinflusst und/oder Veränderungen vorgenommen werden (z. B. durch eigene Software, Netzwerkanbindung, Konfiguration), kann der Integrator als Hersteller eines neuen Systems gelten: In diesem Fall sind die Verpflichtungen des CRA umzusetzen und einzuhalten (z. B. Konformitätsbewertung, CE-Kennzeichnung).

2.2.5 Eigentümer

Der CRA fokussiert sich auf Herstellung und Vermarktung von Produkten und beschreibt daher keine Rolle „Eigentümer“. Da im Eisenbahnsektor der Eigentümer jedoch auch mehrere Rollen einnehmen kann, wird hier auf diese Funktion genauer eingegangen. Die Verpflichtungen aus dem CRA ergeben sich nicht direkt aus der Rolle des Eigentümers, jedoch aus der Verwendung des PDE:

2.2.5.1 Interne Verwendung eines PDE

Wird das Eigentum an einem PDE erworben, um es selbst zu nutzen, so ist der Eigentümer hier als Nutzer zu sehen. Ihm obliegen somit keine Verpflichtungen aus dem CRA. Sollten dem Eigentümer jedoch Schwachstellen oder andere Probleme in dem PDE auffallen, so ist es empfehlenswert diese an den Hersteller zu melden.

2.2.5.2 Vermietung oder Verpachtung eines PDEs

Wenn ein Eigentümer ein PDE vermietet oder verpachtet, stellt er es auf dem Markt bereit und gilt somit im Sinne des CRA als Händler. Damit gelten auch die Verpflichtungen des Händlers, wie zum Beispiel in ↗ CRA Artikel 20 beschrieben, für den Vermieter. Er muss demnach unter anderem prüfen, ob die PDE über eine gültige CE-Kennzeichnung verfügen und er seitens der Hersteller alle erforderlichen Dokumente erhalten hat. **Diese Definition ist von entscheidender Bedeutung** für typische Finanzierungskonzepte von Fahrzeugen.

BEISPIEL

Vermietet z. B. ein Eigentümer aus Serbien (Nicht-EU-Land) Fahrzeuge nach Deutschland, so bringt er diese auf den Markt. Dieser serbische Vermieter muss nun CRA-Konformität sicherstellen.

2.2.5.3 Kostenfreie Überlassung eines Produkts

Analog zur Vermietung eines PDE handelt es sich auch bei einer kostenfreien Überlassung um eine Bereitstellung auf dem Markt. Der Eigentümer ist hier demnach wieder als Händler zu betrachten.

2.2.5.4 Nutzung eines Produkts zur Erbringung von Dienstleistungen

Solang der Eigentümer das PDE selbst verwendet, um Dienstleistungen zu erbringen, erfolgt keine Bereitstellung auf dem Markt wie in ↗ CRA Artikel 3 (22) beschrieben:

Ausnahme: Betreibt ein Eigentümer, der außerhalb der EU ansässig ist, seine PDE auch in der EU, so muss er CRA-Konformität sicherstellen. Diese Regelung hat er bei der Beschaffung zu berücksichtigen. Diese Regelung leitet sich aus dem territorialen Anwendungsbereich des ↗ CRA Artikel 2 (1) „bestimmungsgemäßer Zweck“ ab. Ist geplant, das Produkt in der EU zu betreiben, so muss es CRA-konform sein.

BEISPIEL

Die SBB ist Eigentümer ihrer Zugflotte. Zuggattungen, die in EU-Nachbarländer fahren sollen, müssen den CRA erfüllen.

2.2.5.5 Veränderung eines Produkts und konzerninterne Bereitstellung

Verändert ein Eigentümer das PDE und nutzt es anschließend selbst, stellt er es nicht auf dem Markt bereit und muss so nicht den CRA erfüllen.

Verändert ein Eigentümer das PDE und stellt es innerhalb seines Konzerns einem anderen Unternehmen bereit, so agiert er als Hersteller und muss ↗ CRA Artikel 13 erfüllen.

2.2.6 Betreiber

Die Rolle des Betreibers ist im CRA nicht vorgesehen. Inwiefern sich dennoch Verpflichtungen aus dem CRA für ihn ergeben, hängt davon ab, welche Aufgaben er wahrnimmt:

2.2.6.1 Betrieb von PDE für die Erbringung einer Dienstleistung

Typische Betreiber im Eisenbahnsektor sind Eisenbahninfrastrukturunternehmen (EIU) oder Eisenbahnverkehrsunternehmen (EVU). Das EVU erbringt insbesondere Kundendienste, wie Gütertransport oder Personentransport. In dieser Rolle des Betreibers ist er Nutzer des PDEs und damit Nutzer im Sinne des CRA. Es ergeben sich für ihn keine Verpflichtungen aus dem CRA.

Typische Betreiber im Eisenbahnsektor erfüllen ihre Verpflichtungen gemäß der NIS- und neu NIS-2-Gesetzgebung. Aus diesen Verpflichtungen ergeben sich einige Wechselwirkungen. Folgend sind nur kurz die wesentlichen Aufgaben des Betreibers zusammengefasst und die Beziehung zum CRA genannt.

Nach NIS-2 hat der Betreiber die Verantwortung für den cybersicheren Betrieb der Anlagen zur Aufrechterhaltung der kritischen Dienstleistung. Dafür:

- Führt er Risikoanalysen durch und leitet daraus notwendige prozessuale und technische Maßnahmen ab. Diese Maßnahmen gibt er in Teilen an den Hersteller (Lieferanten) weiter, so dass diese in die Produktentwicklung (Security-by-Design nach CRA) einfließen.
- Überwacht er seine Systeme durch kontinuierliches Monitoring. Durch das Monitoring kann er Angriffe oder Schwachstellen erkennen. Beides nutzt er zur Abwehr, Reaktion und Wiederherstellung der Funktion. Im Eigeninteresse meldet er Angriffe und Schwachstellen an den Hersteller, so dass dieser Hersteller von diesen Angriffen und Schwachstellen Kenntnis erlangt und entsprechende Gegenmaßnahmen (CRA) ergreift.
- Aktualisiert er seine Systeme durch Einspielen verfügbarer Patches der Hersteller (CRA).
- Schult er seine Mitarbeiter und das Management zur anforderungsgerechten Umsetzung der Anforderungen der NIS-2. Dazu gehören auch vertragliche Vereinbarungen mit dem Hersteller (CRA).

2.2.6.2 Betrieb von PDE, die an andere Marktakteure vermietet oder verpachtet werden

Wenn der Betreiber PDE, z. B. Fahrzeuge, betreibt, die von einem Dritten gemietet oder gepachtet werden, um wiederum Dienstleistungen zu erbringen, so kann dies als geldliche oder unentgeltliche Überlassung des PDEs zur zeitweisen Nutzung betrachtet werden. Es handelt sich dabei, wie in ➔ Kapitel 2.4 beschrieben, um eine Bereitstellung auf dem Markt.

Der Betreiber muss in diesem Falle im Sinne des CRA als Händler betrachtet werden.

HINWEIS

Das Befahren von Eisenbahninfrastruktur gegen Trassenentgelte wird nicht als entgeltliche Abgabe gesehen. Hier wird ein Service erbracht. Gleiches gilt für die Nutzung eines Zugs durch einen Fahrgast.

2.3 Definition Produkt

Der CRA macht keine Unterschiede in der Größe oder der Art der Produkte mit digitalen Elementen (PDE). Basierend auf dem CRA gilt jedes in Verkehr gebrachte PDE – egal welcher Integrationsstufe – als Produkt.

DEFINITION

Der CRA gilt für auf dem Markt bereitgestellte **Produkte mit digitalen Elementen (PDE)** deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische physische Datenverbindung mit einem Gerät oder Netz einschließt ↗ CRA Artikel 2 (1).

Das Produkt muss also in irgendeiner Form Daten behandeln und diese über eine Schnittstelle verfügbar machen. Ein PDE enthält demnach mindestens eine Recheneinheit, z. B. Microcontroller und Code, z. B. in Form einer Firmware. Welche Art der Schnittstelle (USB, Ethernet, RS 485, Bluetooth, 5G, ...) zur Anwendung kommt, ist dabei unerheblich. Weiterhin gilt dies auch unabhängig von der Häufigkeit der Nutzung und Menge der übertragenen Daten. Das heißt, es ist unerheblich, ob die Schnittstelle für ständige Kommunikation oder nur als Wartungszugang oder Software-Ladeprozess dienen soll.

Um eine einheitliche Taxonomie im Rail Sektor zu verwenden, wurden die Produkt-Kategorien unter Anwendung der Standards und Gesetze CRA, NIS 2, IEC 63452 und TSI ZZS definiert. Die Definitionen bieten eine Betrachtung aus der Betreiber- bzw. Systemintegrator-Perspektive. Alle Kategorien sind PDE im Sinne des CRA.

„PDE“ im Eisenbahnsektor sind:

Nr.	Kategorie	Beispiele
1	Komponenten	Aktuator, Sensor, Switch, Kamera, ...
2	Fester Satz von Komponenten	Gruppen von Komponenten wie PLC mit E/A-Einheit und Netzgerät
3	Teilsysteme	CCTV-System, RBC, Türsteuerungssystem, Bremssystem, Stellwerk (zentrales System), Feldelementsteuerung, ...)
4	Systeme	Stellwerk (einschließlich Feldelemente, ...), Kraftwerk, Befehls- und Kontrollzentrum, Rollmaterial (Lok, Wagen, ...)

Tabelle 4: Produkte im Sinne des CRA

Von der Definition des Begriffs „PDE“ ausgenommen sind:

Nr.	Kategorie	Beispiele
1	Elemente (nach TSI)	z. B. Zug (Zusammenstellung aus mehreren Rollmaterialien), großer Bahnhof, Tunnel
2	Eisenbahnsystem	Die Zusammensetzung mehrerer Systeme, die den Eisenbahnbetrieb ermöglichen

Tabelle 5: Ausgenommene Produkte im Sinne des CRA

Beispiele dazu können der folgenden ➔ Tabelle 6 entnommen werden.

Produktkategorie	Beispiele
Komponente	■ Aktuator, Sensor, ■ PLC/CPU, E/A-Modul ■ 19" Rack mit Backplane, 19" Karte ■ Router, Schalter ■ Kamera, Radio ■ Einzelner Daten-Rekorder, lokale HMI, Balise
Fester Satz von Komponenten	■ Energie 19" Rack und Karte im Gehäuse ■ Integrierte SPS/CPU + E/A-Modul + Stromversorgung (z. B. Türsteuerungseinheit, HVAC, Bremsensteuerungseinheit, juristischer Ereignisschreiber, Hauptsteuerungs-/Prozessoreinheit, ...) ■ Gleisseitige PLC/CPU + E/A-Modul + Stromversorgung (z. B. lokale Verwaltung von Licht, Wasser, Hochspannungs-Sicherheitseinheit, ...) ■ CCTV (Rekorder + Kameras) ■ Aufzug ■ Branderkennung (lokale Überwachung + Rauchmelder + Rauchventilatoren + Sprinkleranlagen) ■ Redundante Daten-Rekorder, Gruppe von HMIs, Balisen
Funktionales Teilsystem	■ RBC, ETCS-ON-BOARD (EVC+BTM+DMI+...) ■ Logischer Teil des Interlocking ■ Einheiten oder Komponenten in VLANS für 110kV- oder 15kV-Steuernetze ■ TCMS, OMTS, CCS (Fahrzeuge einschließlich fahrzeugseitiger Einheiten) ■ Bahnsteigtüren ■ Integriertes Beleuchtungssystem (zentrale Überwachung + Beleuchtungseinheiten) ■ Integriertes HVAC-System (zentrale Überwachung + eine Reihe von HVAC-Einheiten) ■ Integriertes Brandmeldesystem (zentrale Überwachung + Brandmeldeanlagen)
System	■ Stellwerk, Umspannwerk, Kraftwerk, ■ SCADA-System (einschließlich DMZ, Managementsysteme,..) ■ Rollendes Material, Selbstangetriebene Einheiten ■ CBTC

Tabelle 6: Produktkategorien mit Beispielen

2.4 Bereitstellung und Inverkehrbringen

Das bloße Entwerfen, Entwickeln oder Herstellen eines PDE löst noch keine Pflichten nach CRA aus. Diese Phasen sind zwar wichtig, weil die CRA-Vorgaben das Design und die Produk-

tion beeinflussen, aber erst wenn ein PDE auf dem europäischen Markt in Verkehr gebracht bzw. bereitgestellt wird, greift der konkrete Anwendungsbereich des CRA. Zu diesem Zeitpunkt müssen alle formellen und inhaltlichen Anforderungen erfüllt sein, damit das PDE verkauft werden darf. Daher sollen beide Begriffe im Folgenden kurz erläutert werden.

2.4.1 Inverkehrbringen

Das Inverkehrbringen ist in ↗ CRA Artikel 3 Nr. 21 wie folgt definiert:

DEFINITION

„Inverkehrbringen bzw. in den Verkehr bringen ist die **erstmalige Bereitstellung** eines Produktes mit digitalen Elementen auf dem Unionsmarkt."

Wichtig: Sowohl der Begriff des Inverkehrbringens als auch der Bereitstellung bezieht sich auf **jedes individuelle Einzelprodukt**, nicht auf einen Produkttyp, oder darauf, ob es als Einzelstück oder in Serie hergestellt wurde. Die erstmalige Abgabe des ersten Exemplars einer Produktserie führt wiederum auch nicht die Bereitstellung bzw. Inverkehrbringung für alle weiteren Produkte der gleichen Serie herbei (vgl. Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 ↗ Blue Guide 2022/C 247 Abschnitt 2.2, auch ↗ CRA Erwägungsgrund 38).

Merke: Jedes individuelle Exemplar eines PDE, welches nach dem 11.12.2027 in Verkehr gebracht wird, muss CRA-konform sein!

Der Vorgang des Inverkehrbringens wird vom Hersteller oder von einem Einführer durchgeführt. Wenn ein Hersteller oder ein Einführer ein Produkt zum ersten Mal auf dem europäischen Markt bereitstellt, wird dieser Vorgang rechtlich als „Inverkehrbringen" bezeichnet. Jeder nachfolgende Vorgang, z. B. der Vertrieb zur Weitergabe von einem Händler an einen Vertriebshändler oder von einem Vertriebshändler an einen Endverbraucher, wird als „Bereitstellung" definiert (➔ Abbildung 3).

2.4.2 Bereitstellung

DEFINITION

Die **Bereitstellung auf dem Markt** nach ↗ CRA Artikel 3 Nr. 22 lässt sich in folgende Bestandteile untergliedern, die kumulativ (gleichzeitig) vorliegen müssen:

- Entgeltliche oder unentgeltliche Abgabe
- eines Produkts mit digitalen Elementen ↗ CRA Artikel 3 Nr. 1
- zum Vertrieb oder zur Verwendung
- auf dem Unionsmarkt
- im Rahmen einer Geschäftstätigkeit.

Demnach würde ein Produkt auf dem Markt bereitgestellt, wenn es im Rahmen einer gewerblichen Tätigkeit auf dem Unionsmarkt zum Vertrieb, Verbrauch oder zur Verwendung abgegeben wird, unabhängig davon, ob dies gegen Entgelt oder unentgeltlich geschieht. Zur Auslegung dieser CRA-Definition von Bereitstellung herrscht in der juristischen Literatur allerdings ein

Meinungsstreit. Einer produktsicherheitsrechtlich geprägten Interpretation folgend, wäre die entscheidende Schwelle für die Bereitstellung von PDE die **tatsächlich erfolgte Abgabe** (juristisch „Wechsel der faktischen Verfügungsgewalt"), also der Zeitpunkt an dem das PDE physisch zum Vertrieb oder zur Verwendung durch den Endnutzer geliefert wird und damit die Kontrolle des Herstellers verlässt (sogenanntes „Werkstor-Prinzip"). Da bei Software als PDE eine physische Abgabe nicht zutrifft, wäre hier wiederum die Einräumung der Nutzungsmöglichkeit maßgeblich.

Eine hiervon abweichende Ansicht stellt auf die Festlegung des rechtlich unverbindlichen ↗ Blue Guide 2022/C 247 Abschnitt 2.2 der Europäischen Kommission ab. Eine solche Lieferung umfasst demnach **jedes Angebot** zum Vertrieb, Verbrauch oder zur Verwendung auf dem Unionsmarkt, das zu einer tatsächlichen Lieferung **bereits hergestellter Produkte** führen könnte (z. B. eine Aufforderung zum Kauf oder Werbekampagnen). Es kommt also auf die kommerzielle Absicht und Marktzugang statt auf obigen tatsächlichen Kontrollwechsel über das PDE an. Damit käme es zwangsläufig zu einer früheren Bereitstellung des PDE auf dem Unionsmarkt.

DEFINITION

Dieser Leitfaden empfiehlt, der Auslegung am „Blue Guide" zu folgen. Überzeugend ist hierfür schon die Tatsache, dass es sich bei dem CRA um eine EU-Verordnung handelt, die in allen Mitgliedsstaaten unmittelbar gilt und keiner nationalen Umsetzung bedarf. Hierzu ist ein in den Mitgliedsstaaten möglichst **einheitliches Verständnis** der Anforderungen von großer Bedeutung. Den Leitlinien der Europäischen Kommission, wie dem „Blue Guide", ist daher bei der Deutung besonderes Gewicht beizumessen. Darüber hinaus fielen PDEs nach dieser Auslegung bereits vor Abschluss der physischen Logistik unter die Sicherheitsvorschriften. Sie wäre also nachvollziehbarerweise im Sinne der **Marktüberwachungsbehörden**, die damit **früher**, nämlich bereits bevor das PDE den Endverbraucher erreicht, in die Vertriebskette **eingreifen** und die Einhaltung der Anforderungen des CRA sicherstellen könnten. Klarstellend sei aber betont, dass der **Zeitpunkt** der Erteilung einer **Typzulassung oder Einzelzulassung** insoweit bei beiden Auslegungsvarianten **keine Bedeutung** hat.

Wichtig: Die Übertragung kann entgeltlich oder unentgeltlich erfolgen, was nicht zwingend die physische Übergabe des Produkts erfordert.

Beispiele

In den folgenden Abbildungen sind die Bereitstellung und das Inverkehrbringen anhand von generalisierten Beispielen aufgezeigt.

HINWEIS

In allen Darstellungen ist der Übergang von Hersteller zu Integrator oder zum Nutzer mit einem Pfeil dargestellt. Dies stellt nicht den Zeitpunkt der Lieferung dar. Es ist die Bereitstellung entsprechend Definition in diesem Kapitel, das heißt die Herstellung und das Angebot, gemeint.

→ Abbildung 3 stellt dar, dass jedes Produkt einzeln erstmals auf dem Markt bereitgestellt wird – die Inverkehrbringung – und bei jeder weiteren Veräußerung wieder auf dem Markt bereitgestellt wird. Produktionsserien, Zulassungen oder Ähnliches sind nicht von Belang.

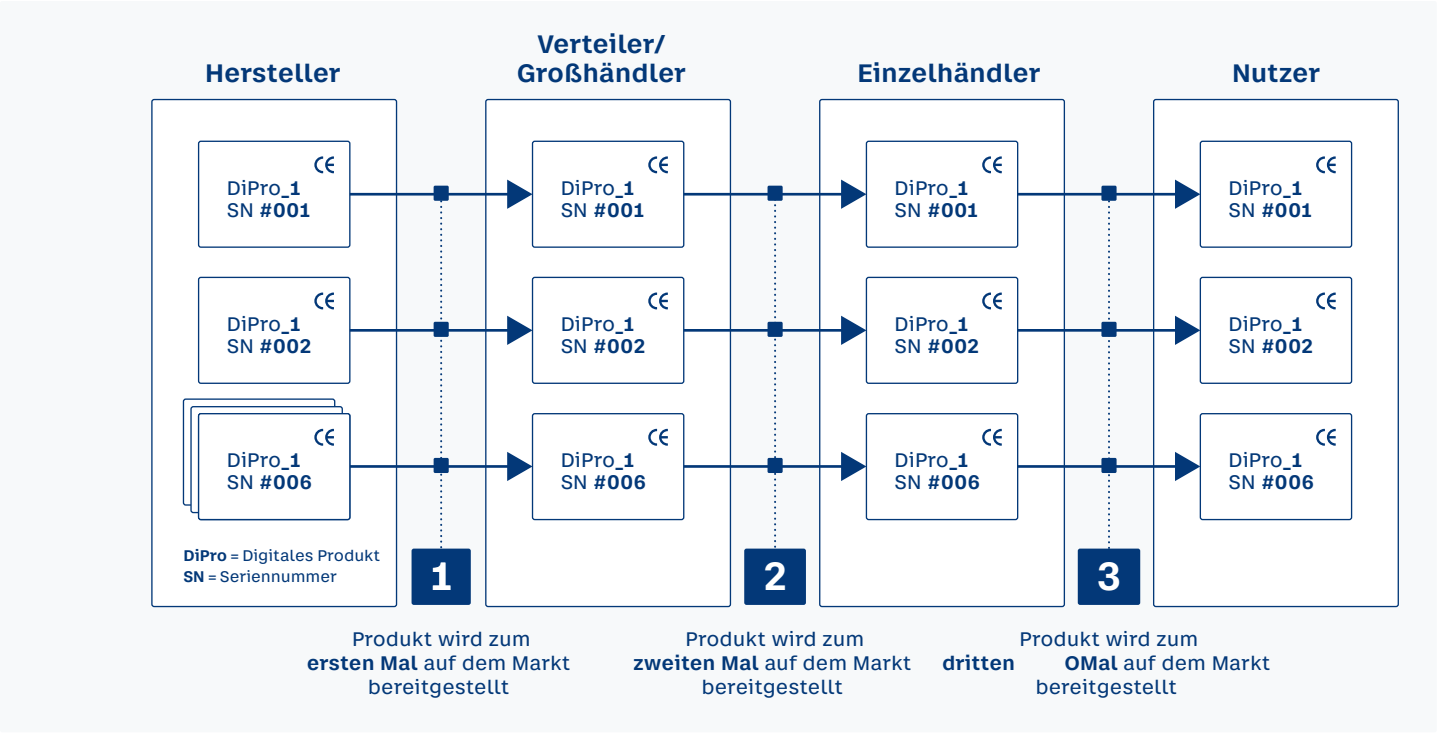

Abbildung 3: Inverkehrbringen mit Integratoren

→ Abbildung 4 stellt dar, dass das Inverkehrbringen vor dem Stichtag des CRA (11.12.2027) keiner Compliance gegenüber dem CRA bedarf. Das gilt für die Herstellung eines einzelnen Produkts wie auch für die Tätigkeit der Integration zu einem neuen Produkt.

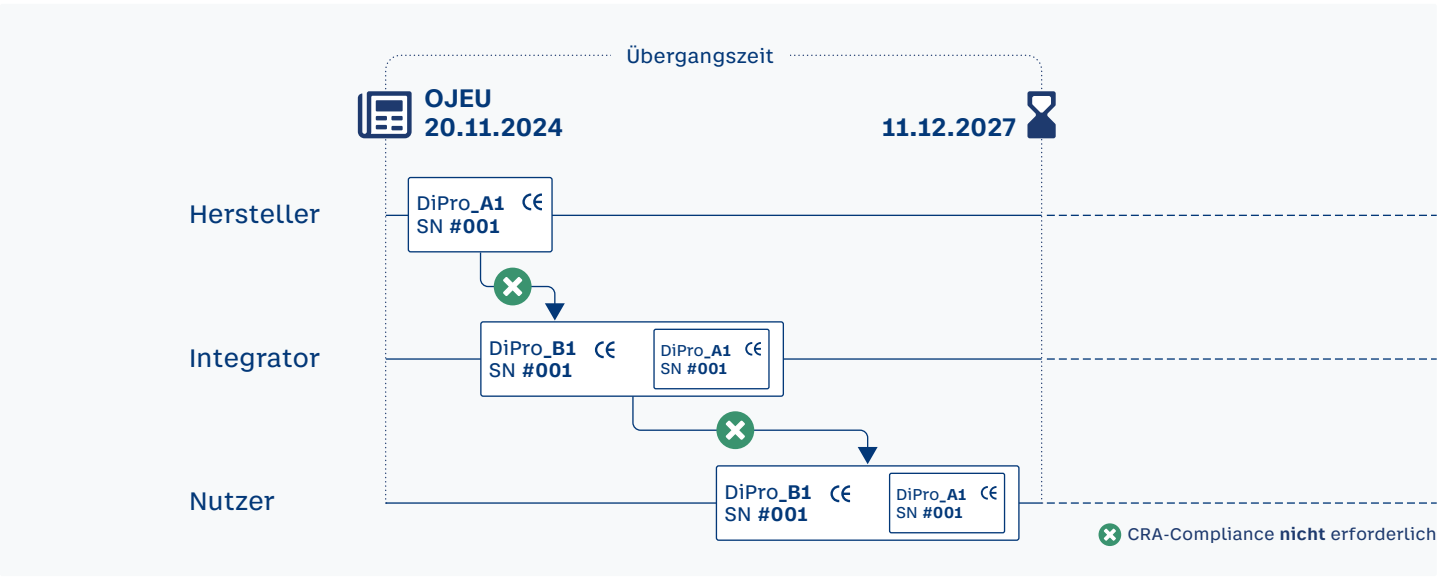

Abbildung 4: Inverkehrbringen vor CRA-Anwendung

→ Abbildung 5 stellt dar, dass die Bereitstellung eines Produkts nach dem 11.12.2027 keine CRA-Konformität erfordert, wenn es bereits vor diesem Datum in Verkehr gebracht (erstmalig bereitgestellt) wurde. Bedingung dafür ist, dass die erneute Bereitstellung ohne substanzielle Veränderung am Produkt erfolgt. Das trifft in der Regel nur auf die Weiterveräußerung durch einen Händler zu.

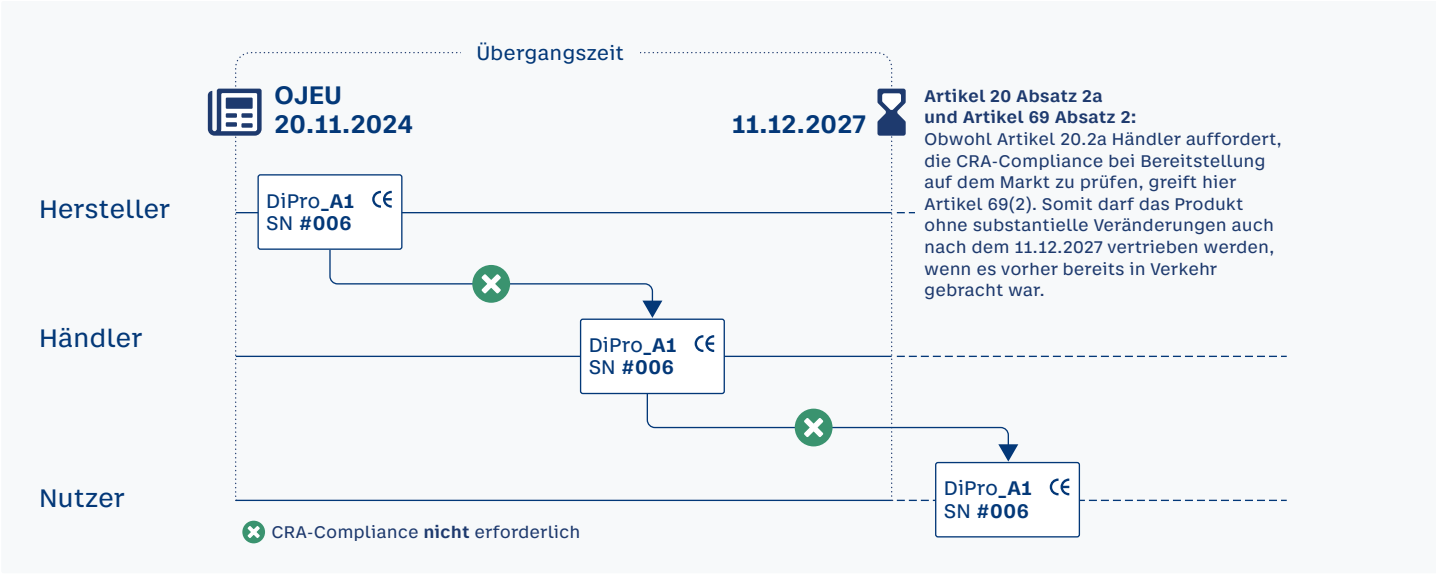

Abbildung 5: Inverkehrbringen vor CRA Anwendung und Distribution ohne Veränderung

➔ Abbildung 6 stellt im Gegenzug zu ➔ Abbildung 5 dar, dass ein Produkt nach dem Stichtag 11.12.2027 nur mit CRA Compliance auf dem Markt bereitgestellt werden kann. Ein Händler ist verpflichtet bei Produkten, die nach dem 11.12.2027 in Verkehr gebracht wurden, zu prüfen, ob sie den CRA erfüllen ↗ CRA Artikel 20 (2a) (2b). Hat der Händler Grund zur Annahme, dass dies nicht der Fall ist, muss vor der Bereitstellung auf dem Markt Abhilfe geschaffen werden. Sollte es ein erhebliches Security Risiko bergen, sind Hersteller und Marktaufsichtsbehörden zu informieren ↗ CRA Artikel 20 (3).

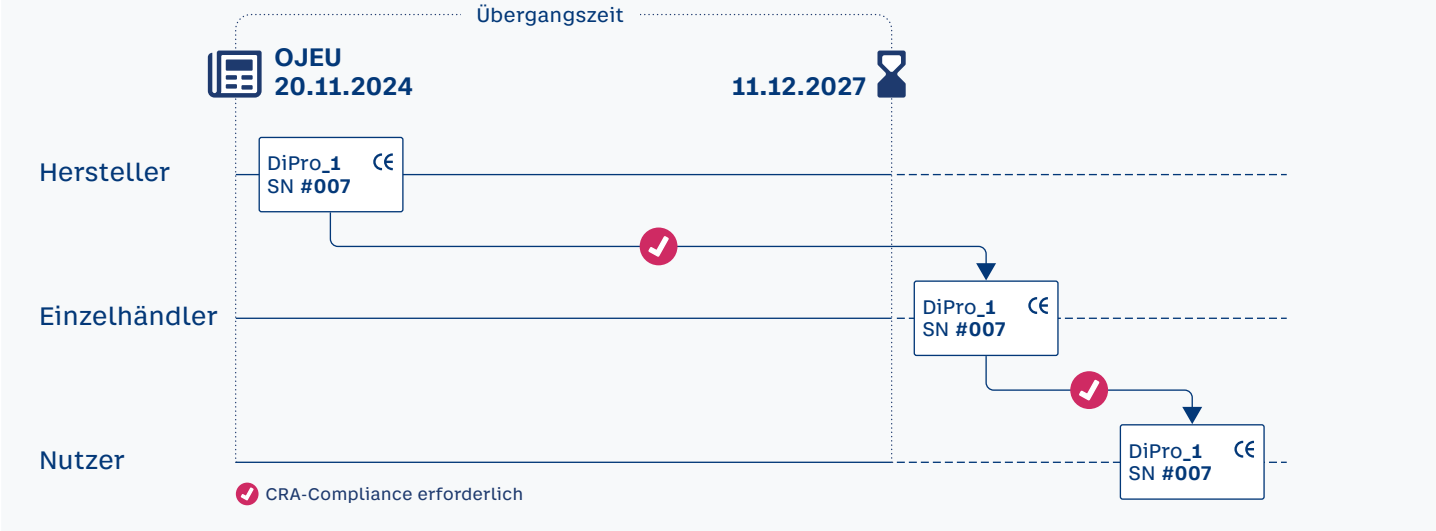

Abbildung 6: Inverkehrbringen und Bereitstellen

➔ Abbildung 7 stellt dar, dass der Integrator Produkte integrieren kann, die vor dem 11.12.2027 in Verkehr gebracht wurden. Stellt der Integrator sein integriertes Produkt dann nach dem 11.12.2027 auf dem Markt bereit (Inverkehrbringung), so muss er die Anforderungen des CRA erfüllen. Er kann dies durch Maßnahmen auf der Integrationsebene sicherstellen. Die Integration von Produkten, die vor dem 11.12.2027 in Verkehr gebracht wurden, stellt somit keine Ausnahmeregelung für den Integrator zur Umgehung des CRA dar.

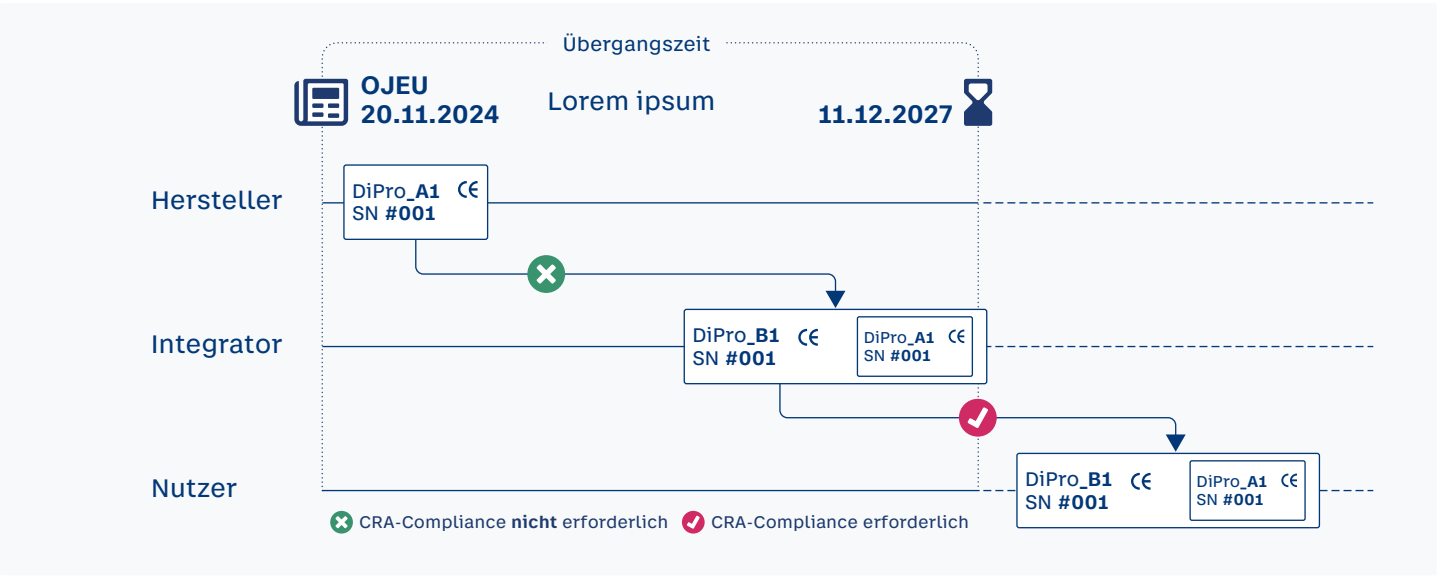

Abbildung 7: Inverkehrbringen in der Migrationsphase

2.5 CRA-Klassen von Produkten

Es lässt sich erkennen, dass der CRA vier allgemeine Produkt-Klassen berücksichtigt. Je nach Klasse gelten unterschiedliche Anforderungen zum Nachweis der CRA Compliance. Der CRA definiert für die drei „spezifischen" Klassen **Wichtige Klasse I, Wichtige Klasse II** und **Kritisch**, welche Produktgruppen darunterfallen. Alle anderen Produkte sind automatisch in der **Standard/Default**-Klasse. Aus diesem Grund gelten alle typischen Rail-Produkte automatisch als Standard/Default, außer sie sind durch den CRA explizit als eine der drei „spezifischen" Klassen definiert.

In ➔ Tabelle 7 sind die Zuordnungen und Anforderungen übersichtlich zusammengefasst. Detaillierte Beschreibungen der Produktkategorien sind in ↗ (EU) 2025/2392 enthalten.

Klasse	Default/Standard	Wichtige Klasse I	Wichtige Klasse II	Kritisch
Definition	Alle Produkte, die nicht unter die drei anderen Klassen fallen	In Anhang III definierte Produkte Klasse I	In Anhang III definierte Produkte Klasse II	In Anhang IV definierte Produkte
Art des Nachweises	■ Selbsteinschätzung ■ Bewertung durch Dritte, wenn die Anforderungen an die Selbstbewertung nicht erfüllt sind**	■ Bewertung durch Dritte* ■ Selbsteinschätzung, wenn harmonisierter Standard angewendet werden kann	■ Bewertung durch Dritte*	■ Bewertung durch Dritte*
Produkte	Jedes andere Bahnprodukt, z. B. ■ RBC (Radio Block Center) ■ EVC (European Vital Computer) ■ Stellwerk (Zentraleinheit) ■ Objekt-Controller ■ Fahrgastinformationssystem ■ Tür-Controller ■ Bremssystem ■ Fahrkartenautomaten ■ Fahrkartensystem ■ System zur Fahrgastzählung ■ Videoüberwachungssystem ■ DMI ■ TCMS ■ Management-System für Zuginformationen ■ HVAC ■ Rollendes Material ■ CBTC ■ ...	■ IAM, PKI, KMC ■ Antivirus ■ SIEM (Security Information and Event Management) ■ Netzwerk-Produkte: VPN, Netzwerkverwaltungs-system ■ Bootmanager ■ Betriebssysteme ■ Mikroprozessoren und Steuerungen mit security-relevanten Funktionen ■ ASIC+FPGA mit srf*** ■ Router/Modems für die Internetanbindung	■ Firewalls, IDS, IPS ■ Hypervisoren, ■ Container ■ Manipulationssichere Mikrocontroller/Prozessoren	■ Hardwaregeräte mit Sicherheitsboxen ■ (z. B. HSM, TPM) ■ Intelligente Zähler-Gateways (intelligente Zähler von Lokomotiven sind nicht enthalten!) ■ Smartcards oder ähnliche Geräte, einschließlich sicherer Elemente *Anmerkung: Mit „kritisch" meint die CRA „cyber-kritisch". Sie bezieht sich nicht auf die Kritikalität im Sinne der Verfügbarkeit für den Betrieb.*

Tabelle 7: Produktklassen, Eigenschaften, Zuordnung

* Ausführliche Informationen über die möglichen Bewertungsmethoden sind in Artikel 32 und Anhang VIII enthalten.
** Die Anforderungen, die für die Selbstbewertung erfüllt werden müssen, sind in Anhang VIII Teil I festgelegt.
***Security-relevante Funktionen

DEFINITION

Kritisch im Sinne des CRA bedeutet ausschließlich „cyberkritisch“. Diese Definition bezieht sich explizit **nicht** auf die Kritikalität im Sinne der Verfügbarkeit für den Betrieb.

HINWEIS 1

Die Europäische Kommission hat am 28.11.2025 einen Durchführungsrechtsakt (EU) 2025/2392 über die technische Beschreibung der Kategorien von wichtigen und kritischen Produkten mit digitalen Elementen veröffentlicht. Dieser tritt am 18.12.2025 in Kraft.

HINWEIS 2

„Cyberkritisch“ ist die Zusammenfassung der Definition aus Erwägungsgrund 46: „Die in dieser Verordnung festgelegten Kategorien kritischer Produkte mit digitalen Elementen sind mit einer Cybersicherheitsfunktion verbunden und werden für eine Funktion verwendet, die ein beträchtliches Risiko nachteiliger Auswirkungen birgt, was ihre Tragweite und ihre Möglichkeit anbelangt, eine große Zahl anderer Produkte mit digitalen Elementen zu stören, zu kontrollieren oder zu schädigen, indem sie direkt manipuliert wird.“

2.6 Keine Vererbung von Merkmalen

Die Klasse eines PDE wird durch ihre Kernfunktion definiert. Wie in ➔ Kapitel 2.5 definiert, können PDE in unterschiedliche Klassen gruppiert werden. Sie können in PDE integriert werden und dadurch unterschiedliche Kernfunktion aufweisen. Es ist jedoch nicht so, dass sich die Klassifikation eines PDE auf die Klassifikation eines anderen PDE – auch wenn es dieses integriert – auswirkt.

DEFINITION

Es wird keine **Vererbung** von Klassen der PDE angewendet. Das heißt, die identifizierte Klasse eines PDE hat keine Auswirkung auf eine Sub-Komponente oder die folgende Integration des PDE. Jedes PDE wird basierend auf der Kernfunktion klassifiziert ↗ CRA Artikel 7 (1).

Das folgende einfache Beispiel ➔ Tabelle 8 anhand des Radio Block Center (RBC) soll dies verdeutlichen. Ein RBC kann aus mehreren Komponenten bestehen, die zu verschiedenen Klassen gehören. Das RBC selbst gehört dabei weiterhin zur Klasse Standard/Default:

Einheit/Teilsystem	Produktklasse
CPU (ohne Sicherheit)	Standard
TPM	Kritisch
Firewall	Wichtige Klasse II
Netzwerkgerät	Wichtige Klasse I
Operating System (OS)	Wichtige Klasse I
Safety-Anwendung (Euroradio)	Standard

Tabelle 8: Beispiel „keine Vererbung der Klassen“

In der folgenden → Abbildung 8 wird ein Beispiel-Schienenfahrzeug mit den verschiedenen integrierten Produktklassen dargestellt. Daran wird noch einmal deutlich, dass es keine Vererbung von Produktklassen gibt.

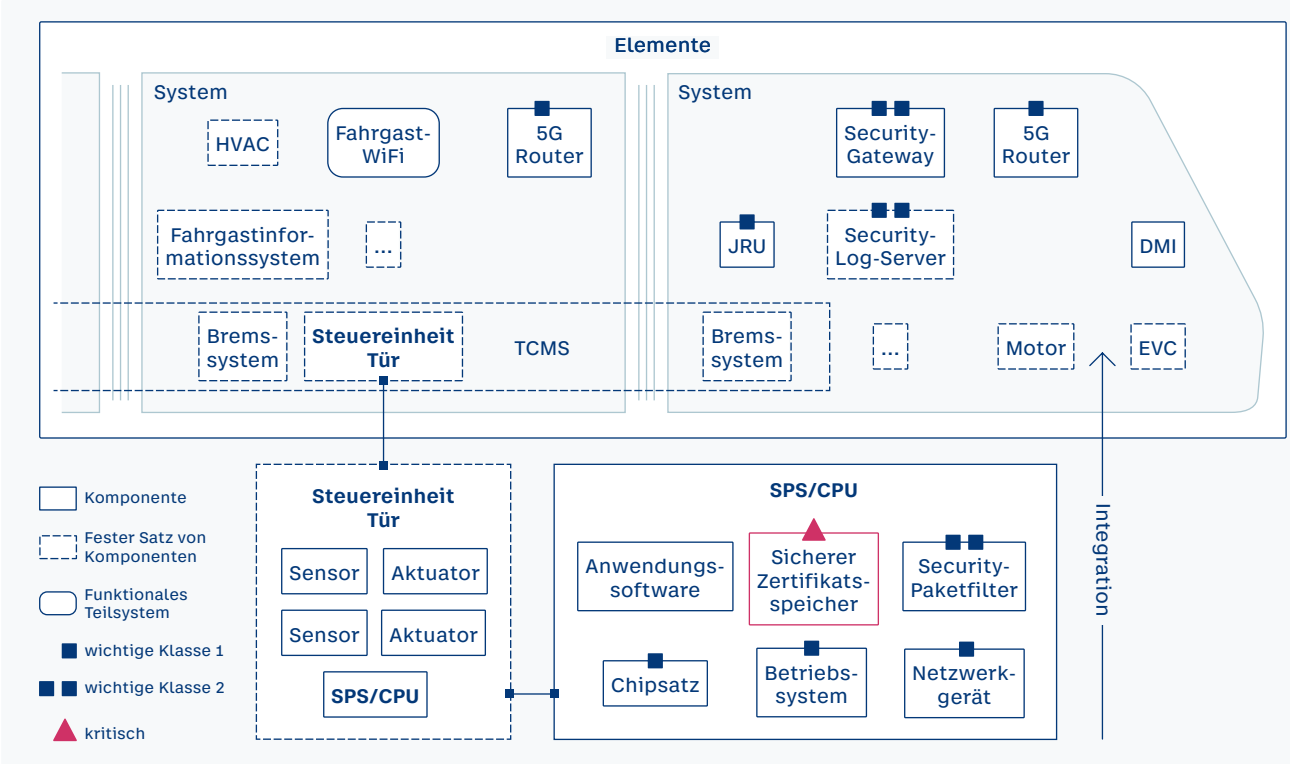

Abbildung 8: Beispiel Zug verschiedene Klassen ohne Vererbung

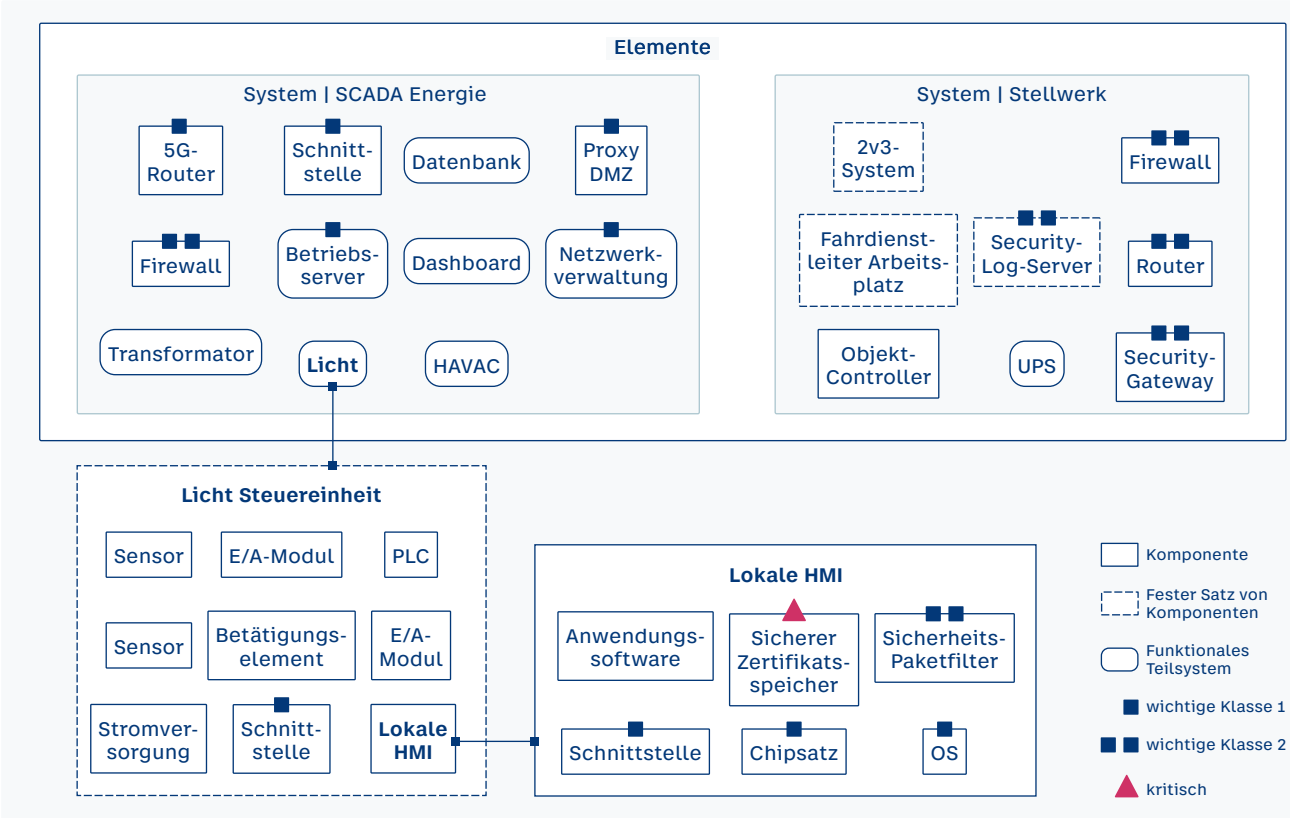

Abbildung 9: Beispiel Infrastruktur: verschiedene Klassen ohne Vererbung

2.7 Anwendung CRA auf das Produkt

Der CRA hat im ↗ CRA Artikel 13 detaillierte Anforderungen, deren Erfüllung für PDEs aller Klassen eine Voraussetzung ist, damit das PDE als CRA-Konform gelten kann. Diese Regelungen sind hier kurz zusammengefasst, um einen Überblick zu geben:

1. Mit Inverkehrbringung bestätigt der Hersteller, dass er das **Produkt** nach den **Cybersicherheitsanforderungen gemäß des ↗ CRA Anhang I Teil I konzipiert, entwickelt und hergestellt** hat.
2. Eine **Risiko-Analyse wurde durchgeführt** und das **Ergebnis** im Design (Konzeption bis Wartung) **berücksichtigt.**
3. Die **Risikoanalyse** wird über den **Nutzungszeitraum aktualisiert** und umfasst den **bestimmungsgemäßen Anwendungsbereich und vernünftigerweise vorhersehbare Verwendung inkl. Umgebungsbedingungen.**
4. Sind **Anforderungen nicht umsetzbar**, wird eine **klare Begründung und Dokumentation** gefordert.
5. Wer **Produkte integriert** (wieder zu Produkten) muss sorgfältig wählen und bewerten. Das **neue Produkt** muss den **CRA erfüllen**.
6. Wird eine **Schwachstelle erkannt/bekannt**, ist diese umgehend an die Stelle zu melden, der diese Komponente **herstellt oder wartet und zu beheben**. Das gilt auch für Schwachstellen in **Open Source Software.**
7. Die **Cybersicherheitsrisiken** und **Schwachstellen** sind **angemessen über den Lebenszyklus zu dokumentieren**.
8. Über den **Produktlebenszyklus und Unterstützungszeitraum** muss der Hersteller für die **Behandlung von Schwachstellen** und **Erfüllen der Anforderungen nach ↗ CRA Anhang I Teil I Sorge tragen.**
9. Die **Updates müssen für 10 Jahre nach Bereitstellung verfügbar bleiben.**
10. Wird eine Software aktualisiert (neue Version), kann die Garantie nach (8) durch den Hersteller auf diese Version beschränkt werden, wenn er kostenfrei die Aktualisierung auf die neue Version bereitstellt.
11. Es können öffentliche Software-Archive bereitgestellt werden, um den Zugang für den Nutzer zu vereinfachen.
12. Die technische **Dokumentation nach ↗ CRA Artikel 31 und Konformitätsbewertung nach ↗ CRA Artikel 12** ist **vor Inverkehrbringung** durchzuführen (self-assessment oder third-party)
13. Die **Aufbewahrung** der technischen Dokumentation und EU-Konformitätserklärung muss **mind. 10 Jahre oder für die Dauer des Unterstützungszeitraums** nach Inverkehrbringung erfolgen.
14. Die **Sicherstellung der Konformität bei Serienherstellung** muss **in geeigneter Weise** erfolgen. Die Berücksichtigung etwaiger Änderungen (Herstellungsverfahren, Konzeption, Normen, ...) muss in angemessener Weise erfolgen.
15. Das Produkt trägt eine Typen-, Chargen- oder Seriennummer ODER (falls nicht möglich) die Informationen liegen als Unterlagen oder der Verpackung bei.
16. Die Angabe von Handelsname und Kontaktdaten muss in geeigneter Weise erfolgen.
17. Der **Hersteller benennt** eine **zentrale Anlaufstelle** zur schnellen und **direkten Kommunikation des Nutzers**, auch zur Schwachstellenmeldung. Die Stelle muss durch Nutzer leicht ermittelt werden können.
18. Es muss sichergestellt werden, dass die Angaben nach ↗ CRA Anhang II in geeigneter Form und Sprache zur Verfügung stehen.

19. Die Angabe des Enddatums des Unterstützungszeitraums erfolgt in leicht zugänglicher Form (Produkt, Verpackung, digital) für Nutzer. Sofern möglich, soll eine Anzeige am Gerät erfolgen, wenn das Enddatum erreicht ist.
20. Die EU-Konformitätserklärung zum Produkt (Kopie oder vereinfacht mit Link zur vollständigen Erklärung) wird beigefügt.
21. Bei **Bekanntwerden oder Annahme der Nicht-Erfüllung der Anforderungen nach ↗ CRA Anhang I während des Lebenszyklus**, **ergreift** der Hersteller **unverzüglich Korrekturmaßnahmen**, um die Konformität wieder herzustellen oder das Produkt zurückzurufen.
22. Alle notwendigen Unterlagen werden der Marktüberwachungsbehörde auf deren begründetes Verlangen bereitgestellt.
23. Bei Einstellung der Betriebstätigkeit werden die Marktüberwachungsbehörde und die Nutzer (soweit mit allen verfügbaren Mitteln möglich) informiert.
24. Die Kommission kann Format und Elemente der Software-Stückliste festlegen.
25. Die Prüfung der Abhängigkeit der Staaten von Software, kann durch die ADCO[3] beschlossen werden. Hersteller müssen dann die Software-Stücklisten bereitstellen.

HINWEIS

Die wesentlichen technischen Anforderungen für die Entwicklung des Produkts sind, wie in ↗ CRA Artikel 13 (1) referenziert, in ↗ CRA Anhang I Teil I beschrieben.

2.8 Begründete Nicht-Anwendung von Anforderungen

Es kann verschiedene Umstände geben, die eine Umsetzung von Security-Anforderungen nicht erlauben oder nicht erfordern (vgl. ↗ CRA Artikel 13 (2), Anhang I Teil I (2), Erwägungsgrund 55). Gesetzlich direkt nachvollziehbare Gründe sind:

- Der Konflikt mit einer anderen Gesetzgebung, deren Lösung herbeigeführt werden muss.
- Der Konflikt mit einer technisch notwendigen Interoperabilität, die zur Nicht-Einhaltung an eben dieser Schnittstelle führt (siehe auch kompatible Systemerweiterung).

Nicht gesetzlich automatisch gedeckte Gründe sind:

- lange Entwicklungszyklen
- Fortsetzung des Absatzes bestehender Produkte.

In allen Fällen muss der Hersteller folgende Schritte durchführen, wenn bestimmte Cybersicherheitsanforderungen nicht anwendbar sind. Er muss:

- dies in der **technischen Dokumentation** begründen,
- bei der Bewertung des Cybersicherheitsrisikos die Interaktion mit dem bestehenden System berücksichtigen,
- die Risiken, die sich aus dem Verzicht auf nicht anwendbare wesentliche Cybersicherheitsanforderungen ergeben, beherrschen, z. B. durch

3 Information: **ADCO ist eine besondere Gruppe zur administrativen Zusammenarbeit.** Details dazu können im Vorschlag für eine „VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020“ nachgelesen werden.

- Hinzufügen kompensierender Gegenmaßnahmen,
- die Einschränkung des Verwendungszwecks,
- Festlegung von Anforderungen an die Betriebsumgebung,
- die Unterrichtung des Betreibers über Restrisiken.

Das heißt: führen bestimmte grundlegende Anforderungen der CRA zu einer Inkompatibilität mit dem System oder dem Eisenbahnsystem, ist eine begründete und dokumentierte Nichtumsetzung der jeweilig betroffenen Anforderung(en) zulässig.

2.9 Änderungen an Produkten

Werden an einem PDE, das bereits in den Verkehr gebracht wurde, Änderungen vorgenommen, so hat dies je nach Art der Änderung und dem Akteur, der die Änderung vornimmt, Auswirkungen auf die aus dem CRA entstehenden Verpflichtungen. Diese Fälle sollen in den nachfolgenden Kapiteln beschrieben werden:

2.9.1 Definition und Anwendung

DEFINITION

Eine **Änderung eines PDEs** laut ↗ CRA Artikel 3 (30) gilt als wesentlich, wenn: sie die vorgesehenen Zweckbestimmung (→ Kapitel 2.9.2) ändert, für den das PDE bewertet wurde, **oder** die Änderung sich negativ auf die Einhaltung der wesentlichen Cybersicherheitsanforderungen der CRA (→ Kapitel 2.9.1) des PDEs auswirkt, beispielsweise durch Vergrößerung der Angriffsfläche.

Die Definition einer wesentlichen Änderung gilt für PDE, die nach dem 11.12.2027 wesentlich geändert wurden, unabhängig davon, wann sie auf den Markt gebracht wurden. Der Begriff ist im CRA nicht immer explizit als „wesentliche Änderung“ formuliert, aber er ergibt sich aus den Anforderungen an den gesamten Produktlebenszyklus und den Pflichten der Hersteller.

Eine Änderung, die ausschließlich dazu dient, das Cybersicherheitsrisiko eines PDEs zu verringern, stellt keine wesentliche Änderung im Sinne des CRA dar, sofern sie keine neuen Funktionen einführt oder den vorgesehenen Verwendungszweck des Produkts ändert (Erwägungsgrund 39). Beispielsweise gelten Security Updates, die bekannte Schwachstellen beheben, nicht **automatisch** als wesentliche Änderungen. Dazu gehört auch die Änderung von Funktionen oder der Leistung eines PDEs, die ausschließlich dem Zweck dient, das Security Risiko zu verringern.

Eine Änderung der Architektur (z. B. durch Hinzufügen neuer Netzwerkverbindungen, Komponenten oder Schnittstellen) ist eine wesentliche Änderung. Dies gilt auch dann, wenn die architektonische Änderung den Verwendungszweck nicht verändert.

Die EU-Verordnung definiert wesentliche Änderungen in ↗ CRA Artikel 3 (30) und in den Erwägungsgründen 38, 39, 40, 41 und 42.

HINWEIS

Weitere Leitlinien für wesentliche Änderungen sollen von der Europäischen Kommission ausgearbeitet und bereitgestellt werden.

Um die fortgesetzte Konformität im Falle einer Produktänderung sicherzustellen, sollte die Einstufung einer Änderung als wesentlich und ihre möglichen Auswirkungen vom Eigentümer der Anlage anhand des folgenden Verfahrens bestätigt werden:

1. Jede Änderung an einem bestehenden PDE ist von dem Unternehmen, das die Änderung vornimmt (i. d.R. vom Hersteller) zu analysieren, um zu überprüfen, ob sie sich auf den bestimmungsgemäßen Zweck des PDEs auswirkt, ob sie sich negativ auf das Security Risiko oder die Einhaltung der „wesentlichen Cybersicherheitsanforderungen“ gemäß ↗ CRA Teil I Anhang I. Wenn mindestens eine dieser Bedingungen erfüllt ist, gilt die Änderung gemäß des CRA als wesentlich.
2. Wenn die Analyse zu dem Ergebnis kommt, dass keine wesentliche Änderung vorliegt, muss das Ergebnis dokumentiert werden. Darüber hinaus muss der Eigentümer der Anlage den Status bestätigen.
3. Wenn die Analyse zu dem Ergebnis kommt, dass eine wesentliche Änderung vorliegt, muss das Unternehmen, das die Veränderung einbringt (i.d.R. der Hersteller) die Konformität überprüfen und sicherstellen, dass das geänderte PDE die grundlegenden Anforderungen des CRA erfüllt. Im Falle einer wesentlichen Änderung wichtiger oder kritischer PDEs (➔ Kapitel 2.9) kann eine neue Bewertung durch Dritte erforderlich sein. Eine wesentliche Änderung an einer Komponente kann sich auf die übergeordnete Ebene (Komponentensatz oder Teilsystem) auswirken und zu einer wesentlichen Änderung auf der übergeordneten Ebene führen (und eine Neubewertung hinsichtlich der CRA-Konformität erforderlich machen). Eine wesentliche Änderung an einer Komponente oder einer festen Gruppe von Komponenten erfordert jedoch nicht automatisch, dass die gesamte Gruppe oder das Teilsystem, in das sie integriert ist, den CRA erfüllt. Der Eigentümer der Anlage muss über das Ergebnis der Analyse informiert werden.

Der Status einer Änderung als „wesentlich“ und ihre definierten Auswirkungen werden vom Eigentümer der Anlage bestätigt.

Die Bestätigung durch den Eigentümer der Anlage bedeutet keine Übertragung der Verantwortung.

HINWEIS

Die Änderung eines PDEs kann sich auf deren Integration in übergeordnete Subsysteme oder Systeme auswirken. Dies muss in der jeweiligen B2B-Beziehung geregelt werden.

2.9.2 Vorgesehene Verwendung

DEFINITION

Gemäß ↗ CRA Artikel 3 (23) ist **die Zweckbestimmung** eines PDEs die Verwendung, für die ein PDE vom Hersteller vorgesehen ist, einschließlich des spezifischen Kontexts und der spezifischen Verwendungsbedingungen, wie sie in den vom Hersteller in der Gebrauchsanweisung, in Werbe- oder Verkaufsmaterialien und -aussagen sowie in der technischen Dokumentation angegebenen Informationen festgelegt sind.

Die wesentlichen Elemente, die die Zweckbestimmung des PDE ausmachen, sind seine **Kernfunktionen** sowie sein **Verwendungskontext** (Anwendungskontext) **und seine Verwendungsbedingungen**. Betrachtet wird ein funktionales Teilsystem, das aus Funktionen besteht:

- Die Änderung einer bestehenden Kernfunktion (einschließlich Konfigurationsaktualisierung) stellt nicht zwingend eine Änderung der Zweckbestimmung dar.
- Das Hinzufügen einer neuen Kernfunktion zum Teilsystem stellt eine Änderung der Zweckbestimmung dar.

HINWEIS

Kernfunktionen beziehen sich auf die Liste der vom PDE bereitgestellten Funktionen. Die gemäß CRA definierte Kernfunktionalität ermöglicht hingegen die Definition der Kategorie von PDEs gemäß ↗ CRA Artikel 2 (1).

In ➔ Tabelle 9 und ➔ Tabelle 10 sind Beispiele von Änderungen (Modifikationen) mit ihren Auswirkungen auf den Zweckbestimmung und Auswirkungen auf die Security aufgeführt.

Beispiel der Modifikation	
Ein TCMS (das die Steuerung und Befehlsausgabe in einem Schienenfahrzeug verwaltet) wird modifiziert (nur Software/Anwendung), ohne dass neue Kernfunktionen oder Komponenten hinzugefügt werden (z. B.: Eine Softwareänderung innerhalb eines Türmanagement-Subsystems, um das Verhalten der Tür zu ändern).	⊖
Ein SCADA-System wird modifiziert (nur Software/Anwendung), ohne dass neue Kernfunktionen oder Komponenten hinzugefügt werden (z. B. Hinzufügen eines neuen Datenpunkts und/oder Symbols ohne Änderung des Prozesses).	⊖
Ein Software-Update zur Integration eines weiteren Punktes oder Signals des bereits vorhandenen Typs im Stellwerk aufgrund geänderter Anforderungen an die Gleisanordnung, ohne dass neue Kernfunktionen hinzugefügt werden und ohne neue Schnittstellentypen.	⊖
Ein TCMS, dem eine neue Hauptfunktion hinzugefügt wurde (z. B.: Hinzufügen eines neuen, vom TCMS verwalteten Teils, wie z. B. kabelgebundene Beleuchtung, die durch ein softwaregesteuertes Beleuchtungsmanagement ersetzt wird)	⊕
Ein SCADA, dem eine neue Hauptfunktion hinzugefügt wird (z. B.: Hinzufügen einer oder mehrerer neuer Zonen für Datenbankserver oder API zu anderen Eisenbahnsystemen)	⊕
Ein Stellwerk erhält ein neues zentrales Diagnosesystem mit Fernzugriffsschnittstelle, das zuvor nicht verfügbar war.	⊕
Ein TCMS, das bereits eine Telemetriefunktion enthält, wird modifiziert (nur Software/Anwendung), um die von der Telemetriefunktion generierten Daten zu verbessern (z. B. Hinzufügen eines neuen Diagnoseberichts aus einer vorhandenen Komponente), ohne neue Verbindung, neue Komponente oder neue Exposition.	⊖ (Safety System, das Telemetriefunktion bereits enthält)
Ein SCADA, das bereits über eine Telemetriefunktion verfügt, wird modifiziert (Ereigniswarnung und -überwachung), um die von der Telemetriefunktion generierten Daten zu verbessern (z. B. Hinzufügen einer neuen Meldung aus einer bestehenden Komponente), ohne dass eine neue Verbindung, eine neue Komponente oder eine neue Exposition erforderlich ist.	⊖ (SCADA, das die Telemetriefunktion bereits enthält)
Eine Aktualisierung der Stellwerkssoftware zur Minderung von Schwachstellen.	⊖
Ein Subsystem wird (wegen Veralterung) modifiziert, ohne dass eine neue Hauptfunktion hinzugefügt wird und ohne dass sich die beabsichtigte Verwendung und Umgebung ändern (z. B. keine neue Architektur, keine neue Exposition).	⊖

⊖ keine Änderung des bestimmungsgemäßen Zwecks ⊕ Änderung des bestimmungsgemäßen Zwecks

Tabelle 9: Beispiele Substantielle Veränderung – Modifikation

Beispiel der negativen Auswirkung auf die Security	Auswirkung Status
Ein TCMS-System erhält eine Remote-Schnittstelle, um z. B. prädiktive Instandhaltung, Remote-Monitoring oder Remote-Software-Update auszuführen	Änderung mit negativer Auswirkung auf TCMS und ggf. alle weiteren angeschlossenen Systeme
Einer bestehenden Kommunikationsschnittstelle wird eine Verschlüsselung hinzugefügt.	Änderung ohne negative Auswirkung
Eine USV im Stellwerk erhält eine Remote-Wartungsschnittstelle, um z. B. prädiktive Instandhaltung, Remote-Monitoring oder Remote-Software-Update auszuführen	Änderung mit negativer Auswirkung auf USV
Remote-Daten-Schnittstelle für Monitoring (read-only) wird an einem Steuerungssystem (z. B. Bremse) integriert. Der Datenabgriff und die Verbindung zum darüberliegenden Steuerungssystem (TCMS) sind nachweislich getrennt (air-gapped).	Änderung mit negativer Auswirkung auf Steuerung ohne Auswirkung auf TCMS

Tabelle 10: Beispiele Substanzielle Veränderung – Negative Auswirkung Security

2.9.3 Anpassungen durch andere Akteure

Wenn ein anderer Akteur als der ursprüngliche Hersteller des PDEs dieses in einer Weise verändert, die von der vorgesehenen Verwendung abweicht, ist dieser Akteur für die Bewertung der Bedeutung der Änderung und gegebenenfalls für die Einhaltung der CRA-Vorschriften verantwortlich.

Ist der Akteur ein Importeur oder Händler und bringt er das geänderte Produkt auf den Markt, wird der Importeur oder Händler zum Hersteller und unterliegt den Verpflichtungen des Herstellers gemäß CRA. Ist der Akteur hingegen ein Endnutzer, wie beispielsweise ein EVU, wird er nicht zum Hersteller, solange er das geänderte PDE nur nutzt und nicht auf den Markt bringt.

In einem solchen Fall, in dem der Endnutzer eine wesentliche Änderung an einem PDE vornimmt, ist der ursprüngliche Hersteller nicht mehr für das geänderte PDE verantwortlich. Die entsprechenden CRA-Verpflichtungen gehen auf das EVU über, falls er das PDE erneut auf dem Markt bereitstellt. Sollte keine Bereitstellung auf dem Markt erfolgen, erlöschen lediglich die Verpflichtungen des Herstellers für das geänderte Produkt. Weiterhin wäre es möglich, mit dem Hersteller einen Supportvertrag zu schließen, in dem der Hersteller sich bereit erklärt, auch weiterhin die Verpflichtungen aus dem CRA zu übernehmen.

Nachfolgende ➔ Abbildung 10 zeigt die Zuständigkeiten in verschiedenen Fällen von PDE-Änderungen durch den Eigentümer der Ausrüstung aufgeführt sind:

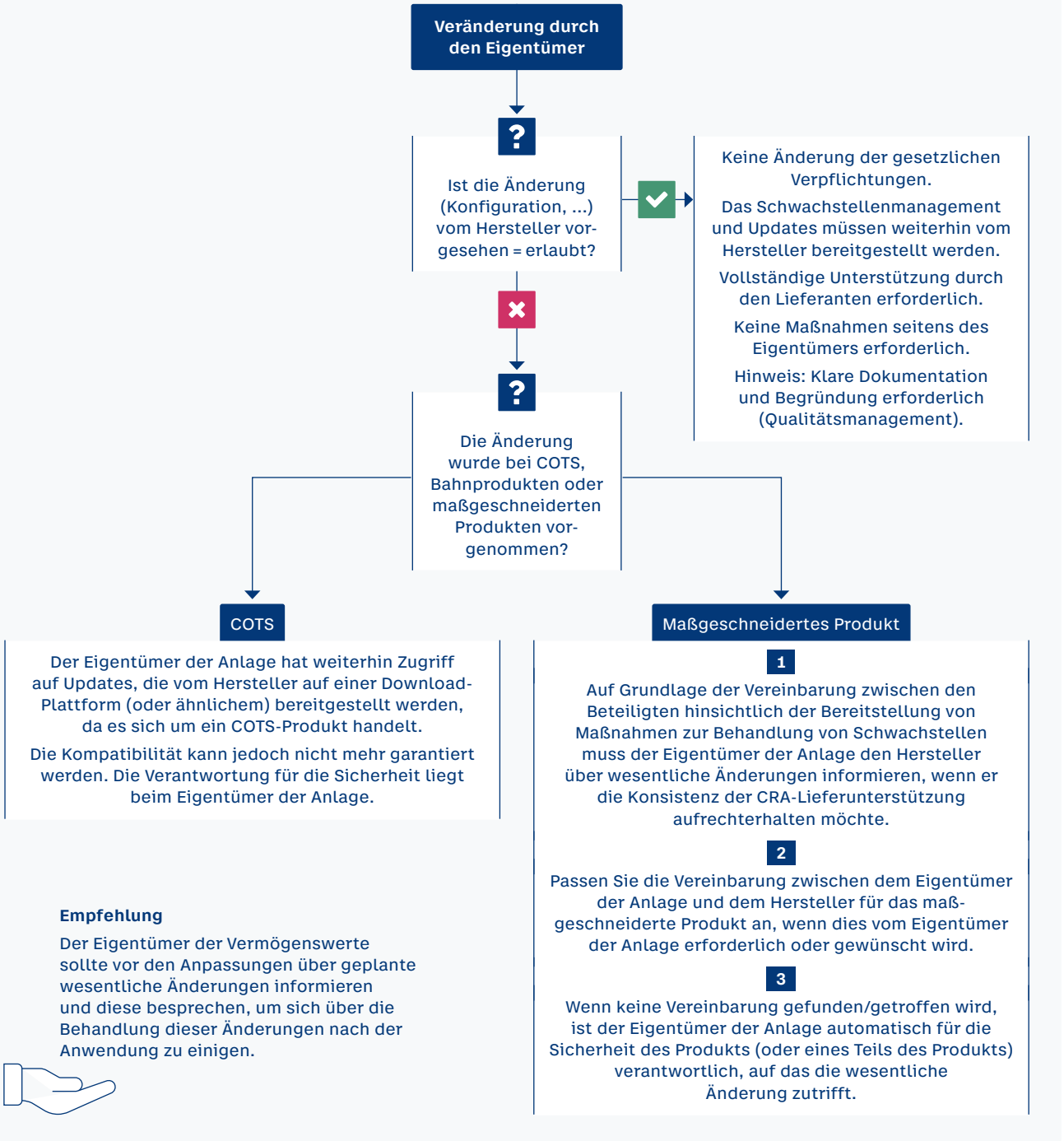

Abbildung 10: Anpassungen durch den Eigentümer

Wenn der Gewährleistungszeitraum noch läuft, sollte der Eigentümer der Anlage den Anbieter über geplante wesentliche Änderungen informieren und diese mit ihm besprechen, bevor sie umgesetzt werden, um sich über den Support für das geänderte Produkt zu einigen.

2.10 Ersatzteile

2.10.1 Definition

DEFINITION

Ersatzteile sind PDEs „die auf dem Markt zum Austausch identischer Komponenten in PDEs angeboten werden und nach denselben Spezifikationen hergestellt werden wie die Komponenten, die sie ersetzen sollen“ ↗ CRA Artikel 2 (6).

Solche Ersatzteile sind vom Geltungsbereich der CRA gemäß ↗ CRA Artikel 2 (6) sowie Erwägungsgrund 29 ausgenommen.

2.10.2 Anwendung

Im Detail können folgende Varianten von Ersatzteilen auftreten und Anwendung finden:

1. **Identische oder „originale“ Ersatzteile**, die genau dieselbe Hardware und Software verwenden wie das Teil, das sie ersetzen.
2. **Ersatzteile mit denselben Funktionen**, die **nur aufgrund von Veralterung neue Hardware und/oder Software** verwenden; Dies sind Ersatzteile, die aus Notwendigkeit geringfügige Änderungen enthalten, wie z. B. den Austausch einer Speicherbank oder einer veralteten CPU durch eine neuere Version, wenn das Original nicht mehr hergestellt wird. Wenn sich das Obsoleszenzmanagement jedoch negativ auf die Einhaltung der wesentlichen Cybersicherheitsanforderungen des CRA durch das PDE auswirkt, beispielsweise durch eine Erhöhung des Risikos oder der Angriffsfläche, findet der CRA Anwendung (siehe Erwägungsgrund 29).
3. **Neu entwickelte oder verbesserte Ersatzteile**, deren **Funktionalität durch Konfiguration** so **eingeschränkt** wurde, dass sie nur die Funktionen des Teils erfüllen, das sie ersetzen, ohne den Verwendungszweck des Teils zu verändern und ohne zusätzliche Bedrohungen oder Risiken für das integrierte Produkt mit sich zu bringen.

HINWEIS 1

Wird ein Ersatzteil für ein neues Produkt oder zur Erweiterung eines bestehenden Produkts eingesetzt, handelt es sich nicht um ein Ersatzteil. Ersatzteile müssen zwingend als solche erkenntlich sein.

Der Hersteller muss eine Deklaration vornehmen, wenn es sich um ein Ersatzteil handelt.

Diese verschiedenen Arten von Ersatzteilen werden bereitgestellt, um die Fortsetzung des Betriebs von langlebigen Systemen im Eisenbahnbereich sicherzustellen.

Ersatzteile, die unter diese Kategorien fallen, können als Ersatzteile ohne Einschränkung hergestellt, auf dem Markt als Ersatzteile angeboten und **im Rahmen der Reparatur bestehender Produkte** eingebaut werden.

Wie in Aufzählungspunkt 3 erwähnt, sind neu entwickelte oder verbesserte Ersatzteile, die neue Funktionen enthalten, nur dann von der CRA-Konformität ausgenommen, wenn sie so konfiguriert sind, dass sie die neuen Funktionen, die im Originalteil nicht vorhanden waren, deaktivieren oder blockieren. Um neue Funktionen nutzen zu können, ist die CRA-Konformität erforderlich. Infolgedessen kann eine solche Komponente als neue CRA-konforme Komponente mit verbesserter Funktionalität und als Ersatzteil mit eingeschränkter Funktionalität verwendet werden. Die Aktivierung der verbesserten Funktionalität zu einem späteren Zeitpunkt ist möglich, wenn die CRA-Konformität über den gesamten Lebenszyklus nachgewiesen und gewährleistet ist.

Als Empfehlung würde die Produktion und Lieferung von CRA-konformen Ersatzteilen, die bereits vor Ablauf der Übergangsfrist (11.12.2027) sowohl als neue Komponenten als auch als Ersatzteile mit eingeschränkter Funktion verwendet werden können, kostspielige Änderungen in späteren Betriebssystemen verhindern und die Anzahl der Ersatzteile reduzieren, die EVU und Zulieferer auf Lager halten müssen. Solche Ersatzteile würden den Übergang bestehender Systeme zur CRA-Konformität erleichtern (➔ Kapitel 2.5).

Der Status eines Ersatzteils in diesem Zusammenhang wird zwischen dem Hersteller und dem Eigentümer der Anlage im Rahmen eines formellen Abnahmeverfahrens vereinbart.

Hintergrund: Diese verschiedenen Arten von Ersatzteilen werden vorgestellt, um den Betrieb von Langzeitsystemen im Eisenbahnbereich zu ermöglichen.

2.11 Projektbasierter Ansatz

Der Eisenbahnsektor ist ein Sektor besonders wichtiger Einrichtungen ↗ NIS2UmsG Anlage 1 S. 44 – wie in der NIS-2-Richtlinie festgelegt – und unterliegt umfangreichen regulatorischen Rahmenbedingungen, um Sicherheit, Interoperabilität und Betriebskontinuität zu gewährleisten. Aufgrund dieser Rahmenbedingungen und der langen Lebensdauer seiner Produkte ist der Sektor durch komplexe, lange Projektzyklen gekennzeichnet, wobei große Infrastruktur- oder Fahrzeugprojekte oft 7 bis 20 Jahre von der Planung bis zur Fertigstellung dauern.

Eisenbahnen funktionieren als Systeme von Systemen – grenzüberschreitend miteinander verbunden und unter Einbeziehung älterer Technologien und neuer digitaler Komponenten – unter der Aufsicht nationaler und europäischer Regulierungsbehörden. Die Einführung der CRA und ihrer Security Verpflichtungen stellt eine Herausforderung für die Branche dar. Es ist jedoch unerlässlich, dass sich alle Beteiligten, einschließlich der Hersteller, auf die neuen Herausforderungen und Risiken einstellen, die mit der zunehmenden Digitalisierung einhergehen. Alle Akteure der Branche müssen ihre Arbeitsmethoden anpassen, um diesen Risiken zu begegnen und Safety und Security in ihren Risikomanagementpraktiken in Einklang zu bringen.

Die einzigartige Betriebs- und Regulierungsstruktur des Eisenbahnsektors funktioniert nach einem projektbasierten Ansatz. Eisenbahnsysteme werden in der Regel als groß angelegte, langfristige Projekte entwickelt und eingesetzt, die eine komplexe Integration von Infrastruktur und Rollmaterial erfordern – oft über nationale Grenzen hinweg. Im Rahmen dieser Projekte werden die Komponenten sorgfältig ausgewählt, zertifiziert und als Interoperabilitäts-

komponenten gemäß den TSI installiert, wobei bewährte Zulassungs- und Sicherungsprozesse zur Gewährleistung der systemweiten Sicherheit und Kompatibilität zum Einsatz kommen.

Die CRA verwendet zwar nicht das Konzept des „Projekts“, sondern befasst sich nur mit einzelnen PDE, doch haben ihre Security Anforderungen erhebliche Auswirkungen auf Projekte. Um die Ziele der CRA und der NIS-2 hinsichtlich sichererer Produkte und Infrastrukturen auf konsistente und praktische Weise zu erreichen, ist es unerlässlich, die Auswirkungen der Rechtsvorschriften auf laufende Projekte zu analysieren und zu steuern. Der Leitfaden definiert daher, wie die Ziele des CRA – insbesondere im Bereich der digitalen Sicherheit – mit dem projektorientierten, sicherheitskritischen Rahmen der Eisenbahnindustrie in Einklang gebracht werden können.

2.11.1 Anwendung

Nach der Einführung gelten die folgenden Regeln für bestehende Projekte, die bis zum 11.12.2024 (Datum des Inkrafttretens der CRA) unterzeichnet wurden.

In jedem Fall gilt weiterhin: Die Verantwortung für die CRA-Compliance verbleibt vollständig beim Hersteller (Lieferanten).

[a] Definition eines bestehenden Projekts

Ein Projekt – wie in diesem Zusammenhang verwendet – ist ein B-2-B-Auftrag zwischen einem Endnutzer und einem Hersteller (einem Systemintegrator oder direkt einem Produktlieferanten), der die Konzeption, Tests und Abnahme umfasst und sorgfältig geplant hat, um die Lieferung einer bestimmten Anzahl von „Produkten“ für den Betrieb, einschließlich Migration/Integration, zu erreichen.

Ein Projekt, das auf einer Anforderungsspezifikation basiert, wird durch eine vertragliche Vereinbarung abgedeckt, in der der Startpunkt (Projektbeginn) und das Ende (Migration/Integration und Ende der Lieferung, einschließlich Gewährleistung/Garantie und eventueller Optionen) festgelegt sind.

[b] Konformität innerhalb eines bestehenden Projekts

Jedes PDE, das nach dem 11.12.2027 in Verkehr gebracht wird, muss CRA-konform sein.

Für bestehende Projekte ausgewählte PDEs erfüllen möglicherweise nicht alle risikobasierten grundlegenden Anforderungen. Aus diesem Grund gilt für bestehende Projekte das folgende Verfahren:

1. Der Hersteller legt eine Risikoanalyse für die Komponente, das Teilsystem oder das System für das bestehende Projekt vor.
2. Jedes PDE enthält eine klare Begründung in der Security Risikoanalyse auf Systemebene sowie eine Analyse des Restrisikos, um den Nutzer zu informieren.
3. Es werden Maßnahmen zur Minderung des anfänglichen Restrisikos vorgeschlagen.
4. Das Restrisiko kann auf Systemebene gemanagt werden.
5. Das Restrisiko muss für den Eigentümer der Anlage akzeptabel sein, und es wird eine gegenseitige Vereinbarung mit dem Nutzer getroffen ➔ Kapitel 2.12.

[c] Einschränkung

Für Projekte, die nach dem 11.12.2024 unterzeichnet werden, darf dieser Ansatz nicht angewendet werden. Stattdessen sollten die wesentlichen Anforderungen des CRA von Anfang an berücksichtigt werden und Security by Design muss als Grundlage für die Einhaltung der CRA-Vorschriften betrachtet werden.

2.12 Mutual Agreement

Die CRA lässt bei der Erfüllung ihrer wesentlichen Cybersicherheitsanforderungen eine gewisse Flexibilität zu. Die (begrenzte) Flexibilität resultiert aus der risikobasierten Auswahl der geeigneten Maßnahmen gemäß ↗ CRA Artikel 13 (2). Wenn jedoch ein PDE oder seine Komponenten die wesentlichen Cybersicherheitsanforderungen der CRA nur teilweise erfüllen, sind Transparenz und Kommunikation zwischen Hersteller und Nutzer (vergleiche Definition Nutzer und Kunde in ➔ Kapitel 2.2.1) unerlässlich.

Beispiele hierfür sind:

- Ersatzteile;
- Komponenten einer CRA-konformen PDE, die während der Übergangsphase gekauft wurden und selbst keine Konformität erforderten;
- Projekte im Eisenbahnsektor, die sich über das Ende der Übergangsphase hinaus erstrecken.

Um sowohl die Risikobewertung des PDE – das heißt die von diesen umgesetzten grundlegenden Anforderungen – als auch die Akzeptanz des Restrisikos durch den Nutzer zu erleichtern, wenn bestimmte grundlegende CRA-Anforderungen für das betreffende PDE nicht umsetzbar sind, sollte das folgende Verfahren beachtet werden:

1. Um das Produkt für die CE-Kennzeichnung vorzubereiten, ist der Hersteller verpflichtet, die Nutzung von Flexibilitäten bei der Anwendung der wesentlichen Anforderungen an den CRA in der technischen Dokumentation, in der Risikobewertung des Produkts und in den Informationen und Anweisungen für den Benutzer zu dokumentieren (Security Anwendungsbedingungen).
2. Hersteller und Nutzer sollten einen Informationsaustausch über folgende Punkte durchführen:
   a. Security-relevante Anwendungsbedingungen für die Security Funktionen, die vom Produkt nicht bereitgestellt werden können;
   b. die Betriebsumgebung des Produkts;
   c. ausgleichende Gegenmaßnahmen, die von dem System bereitgestellt werden, in das das Produkt integriert ist.
3. Hersteller und Nutzer sollten sich über die genannten Punkte gegenseitig abstimmen. Die Vereinbarung sollte formalisiert werden und so schnell wie möglich in Kraft treten. Sie sollte je nach Projektstatus in verschiedenen Phasen anpassbar sein, z. B. während der Angebotsphase Klausel für Klausel, während der Konzeption und Entwicklung durch Genehmigung der Dokumentation oder durch Änderungsmanagement. Der Security Case

kann eine gültige Grundlage für diese formelle Abnahme sein (Security Case derzeit nach TS 50701, zukünftig IEC 63452).

HINWEIS

Der Security Case kann bereits in einer frühen Projektphase erstellt und regelmäßig an Entwicklungen im Projekt angepasst werden.

- **Die gegenseitige Vereinbarung ist nicht als Übertragung der Verantwortung vom Hersteller auf den Nutzer zu verstehen**. Jede Partei bleibt für ihre jeweiligen Verpflichtungen im Rahmen der vertraglichen und gesetzlichen Bestimmungen verantwortlich.
- Die Vereinbarung kann nicht automatisch auf andere Nutzer (Kunden) oder zukünftige separate Transaktionen ausgeweitet werden. Als solche erlaubt sie dem Hersteller nicht, das Produkt ohne Begründung für die genutzten Flexibilitäten und ohne entsprechende gegenseitige Vereinbarung mit den genannten Nutzern allgemein auf dem Markt für andere Nutzer verfügbar zu machen.

2.13 Maßgeschneiderte Produkte

Für maßgeschneiderte Produkte können die folgenden Ausnahmen von der allgemeinen CRA-Konformität gelten:

- Gegenseitige Vereinbarung über die Kosten von Software-Updates anstelle der Verpflichtung zur kostenlosen Lieferung ↗ CRA Anhang I Teil II (8)
- Verzicht auf die „sichere Standardkonfiguration“ und „Zurücksetzen auf Standard“ ↗ CRA Anhang I Teil I (2b)

Ein maßgeschneidertes Projekt ist im Erwägungsgrund 64 als *„für einen bestimmten gewerblichen Nutzer auf einen bestimmten Zweck zugeschnitten“* definiert. **Daraus können folgende spezifische Beispiele für den Bahnbereich abgeleitet werden:**

DEFINITION

Ein Produkt ist maßgeschneidert, wenn: das Produkt auf der Grundlage einer kunden-spezifischen Spezifikation/Anforderung entwickelt wird, so dass zusätzliche Design/Entwicklungs-Tätigkeiten notwendig sind.

Ein Produkt ist nicht allein deshalb maßgeschneidert, weil

- Parameter geändert werden (z. B. Auswahl der Funktionalität nach verfügbaren Parametern des Produkts),
- Konfigurationsänderungen, die in einem vordefinierten Bereich liegen oder keine individuellen Prozesse auf Nutzer- oder Herstellerseite erfordern,
- ein Produkt auf der Grundlage von TSI, ERJU System Pillar oder EULYNX entwickelt wird,
- Verfügbare Produkte werden projektspezifisch zusammengestellt, wobei die Standardfunktionen des Produkts genutzt werden, sodass keine Konstruktions-/Entwicklungsarbeiten erforderlich sind (z. B. eine SPS mit E/A-Modulen oder eine Unterstation mit unterschiedlicher Anzahl derselben Kurzschluss-Trennvorrichtungen).

Ein Produkt, das in einem **Katalog** eines Herstellers enthalten ist und bestellt werden kann, kann als **COTS** betrachtet werden. Das trifft üblicherweise für Standard-Produkte, wie Firewall, IDS, IPS, Switches, Router, etc. zu.

Darüber hinaus gelten die folgenden Kriterien, um festzustellen, ob ein Produkt maßgeschneidert ist:

Ein Produkt **ist nicht allein aufgrund** der folgenden Faktoren maßgeschneidert:

- Änderungen der Parameter (z. B. Auswahl der Funktionalität durch eine im Produktdesign enthaltene Konfiguration);
- Änderungen der Konfiguration, die innerhalb eines definierten Bereichs liegen oder keine kundenspezifischen Prozesse seitens des Herstellers erfordern;
- Entwicklung des PDEs nach Standards wie TSI, ERJU System Pillar oder EULYNX;
- Kombination verfügbarer PDEs auf projektspezifische Weise, solange die Standardfunktionen des Produkts genutzt werden und keine Konstruktions-/Entwicklungsarbeiten erforderlich sind (z. B. eine SPS mit E/A-Modulen oder eine Unterstation mit unterschiedlicher Anzahl derselben Kurzschluss-Trennvorrichtungen).

Ein Produkt **sollte nicht** allein aufgrund von Änderungen am mechanischen Design oder an der Hardware als maßgeschneidert betrachtet werden, wenn diese Änderungen keine Auswirkungen auf die Software oder die Konfiguration und damit auf die Verpflichtungen zur Bereitstellung von Schwachstellenmanagement und Security Updates haben, z. B.:

- Ersetzen eines 24-Zoll-Displays durch ein 28-Zoll-Display mit derselben Auflösung;
- Hinzufügen einer redundanten anstelle einer einzelnen Stromversorgung (z. B. für einen Server).

Im Allgemeinen sind PDE-Kategorien, die in den Anhängen III-IV der CRA als „wichtig Klasse I“, „wichtig Klasse II“ oder „kritisch“ aufgeführt sind, nicht als maßgeschneidert anzusehen, da sie COTS-Netzwerkprodukte (Modems, Switches, Router ...), Security Produkte (Firewalls, IDS, IPS, EDR/XDR, AV, IAM, PKI, SIEM, HSM ...), Betriebssysteme, Hypervisoren, sichere Mikrocontroller, Smartcards und SPS darstellen. Ausnahmen sind möglich.

Ebenso sollte jedes PDE, das in einem Katalog (z. B. Produktangebot + Preis) eines Herstellers aufgeführt ist, als COTS betrachtet werden.

Da **der CRA die Bereitstellung von Security Updates für maßgeschneiderte Produkte** gegen eine Gebühr anstelle einer kostenlosen Bereitstellung zulässt, sind die folgenden Verfahren festgelegt:

- Der Status „maßgeschneidert“ muss vom Hersteller begründet und vom Eigentümer der Anlage akzeptiert werden. Diese Akzeptanz ist eine Voraussetzung für den Vertragsabschluss.
- Der Hersteller ist verpflichtet, Schwachstellen, die in seinen Produkten auftreten, während des Unterstützungszeitraums zu beheben. Die Kosten für die Behebung dieser Schwachstellen sind einvernehmlich zu vereinbaren, einschließlich Bedingungen wie Aktualisierungshäufigkeit und Supportzeitraum im Servicevertrag.

- Der Hersteller muss sich im Servicevertrag auf eine Standard-Aktualisierungshäufigkeit für Security Updates für geschäftliche Berechnungszwecke (z. B. 6 Monate) einigen.

Die Erfüllung einer Supportdauer kann auch durch geplante Hardware- oder Software-Ersatzbeschaffungen erfolgen. Dies kann beispielsweise für ein komplexes System wie ein Fahrzeug mit regelmäßigem Austausch von Komponenten (z. B. kritische COTS-Produkte) mit einem kompatiblen Supportzeitraum gelten. Es ist möglich, dass der Eigentümer der Anlage nach dem Austausch die ausgetauschten Produkte unabhängig vom Hersteller des komplexen Systems verwaltet.

2.14 Kompatible Systemerweiterung

2.14.1 Definition

Kompatible Systemerweiterungen sind notwendig, um bestehende Systeme mit neuen Systemen verknüpfen zu können. Die „Gestattung“ kompatibler Systemerweiterungen erfolgt dabei basierend auf der Möglichkeit gewisse Security Anforderungen begründet nicht anzuwenden → Kapitel 2.8.

DEFINITION

Eine Kompatible Systemerweiterung ist eine neue Einheit, Teilsystem oder System, das zu einem bestehenden System oder Eisenbahnsystem hinzugefügt wird, das mit bestehenden Systemen oder Eisenbahnsystemen interagieren muss und daher seiner Natur nach mit bestehenden Systemen oder Eisenbahnsystemen an externen Schnittstellen interoperabel sein muss.

2.14.2 Nutzen und Regelung

Durch die Definition in Verbindung mit → Kapitel 2.8 können „veraltete“ Schnittstellen weiterhin Anwendung finden, um die Kompatibilität sicherzustellen. Unbenommen von dieser Regelung bleibt der Grundsatz, dass die neu hinzugefügten PDE CRA-konform sein müssen und für die Abweichung die Schritte nach → Kapitel 2.8 umzusetzen sind.

BEISPIEL

Beispiele dafür können sein:

- Stellwerk-Stellwerk-Schnittstelle
- Integration ETCS in bestehende Schienenfahrzeuge
- Integration Fahrgastinformationssystem in bestehende Schienenfahrzeuge
- Anbindung Stellwerk an bestehendes Dispositionssystem
- Erweiterung eines bestehenden Triebzugs um einen Mittelwagen → Kapitel 4.1.6

2.14.3 Anwendung

Wenn eine Vorschrift (z. B. eine TSI) oder das Vorhandensein von Altsystemen erfordert, dass das PDE Schnittstellen verwendet, die nicht vollständig mit den einschlägigen Anforderungen der CRA-konform sind, muss der Hersteller folgende Maßnahmen ergreifen:

1. Eine Begründung in der technischen Dokumentation vorlegen. Akzeptable Begründungen sind:
   a. Verpflichtungen zur Interoperabilität, die sich aus TSI oder anderen EU-Rechtsvorschriften ergeben.
   b. Die Notwendigkeit, veraltete Normen zu befolgen, um die Kompatibilität mit bestehenden Systemschnittstellen zu gewährleisten, da das Produkt mit digitalen Elementen (PDE) ohne diese Maßnahme nicht in der Lage wäre, seine beabsichtigte Funktion zu erfüllen. In der Security Risikoanalyse bewerten, wie das betreffende PDE mit dem bestehenden System und mit dem Eisenbahnsystem insgesamt interagiert.
2. Beheben aller Risiken, die sich aus Teilen ergeben, die einigen der wesentlichen Cybersicherheitsanforderungen nicht entsprechen, beispielsweise durch:
   a. Hinzufügen von kompensierenden Gegenmaßnahmen;
   b. Einschränken des vorgesehenen Verwendungszwecks des PDEs;
   c. Festlegen zusätzlicher Anforderungen an die Betriebsumgebung;
3. den Eigentümer der Anlage über die gewählten Maßnahmen (a-c) und die daraus resultierenden Restrisiken informieren.

In jedem Fall gilt dieser Ansatz nur für die Interoperabilitätsschnittstelle. Dies hat keine Auswirkungen auf die Konstruktion des restlichen PDEs.

Es folgt eine Liste mit Beispielen für kompatible Systemerweiterungen:

- Neuer Wagen in einem Zugverband, der mit dem Rest des bestehenden Zugverbands interagieren muss;
- Neuer Wagen, der mit einer bestehenden Flotte kompatibel sein muss;
- Neue Eurobalise auf einer ETCS-Strecke, die mit den Bordrechnern der bestehenden Flotte interagieren muss;
- Bordrechner eines neuen Zuges auf einer bestehenden ETCS-Strecke, der mit den bestehenden Eurobalises und RBC entlang der Strecke interagieren muss;
- Neuer Bahnhof einer U-Bahn-Linie, der mit dem bestehenden Signalsystem und der bestehenden Flotte interagieren muss;
- Neue Infrastruktur für ein nationales Zugsteuerungssystem, die mit der bestehenden Flotte interagieren muss;
- Neuer Zug mit der neuesten Baseline für fahrzeugseitige Geräte, der mit dem bestehenden nationalen Zugsteuerungssystem interagieren muss;
- Anschluss eines Industriekomplexes an eine bestehende Eisenbahnstrecke, der mit dem bestehenden Signalsystem und der bestehenden Flotte interagieren muss;
- Neues Nebengleis zu einer bestehenden Eisenbahnstrecke, das mit dem bestehenden Signalsystem und der bestehenden Flotte interagieren muss.

Es ist wichtig zu betonen, dass alle neuen kompatiblen Systemerweiterungen, die nach dem 11.12.2027 auf den Markt kommen, vollständig CRA-konforme PDEs sein werden. Sie werden

jedoch über Legacy-Schnittstellen und -Protokolle mit älteren bestehenden Geräten interoperabel sein.

Anwendungsbeispiele zur kompatiblen Systemerweiterung sind in ➔ Kapitel 4.1.6 dargestellt.

2.15 Meldepflichten

Die Meldepflichten unterscheiden sich nach Art des Ereignisses oder der Schwachstelle und nach Produkteinführungsdatum. In den folgenden Kapiteln sind die Verpflichtungen aufgeführt. Weitere Beschreibungen und Hilfestellungen, wie dies praktisch umgesetzt werden kann sind in ➔ Kapitel 3 aufgeführt.

2.15.1 Einleitung

Für den leichten Informationsaustausch zu aktiv ausgenutzten Schwachstellen sowie schwerwiegenden Sicherheitsvorfällen wird eine neue zentrale Meldeplattform etabliert.[4]

Alle aktiv ausgenutzten Schwachstellen und schwerwiegende Sicherheitsvorfälle, die sich auf die Security von Produkten mit digitalen Elementen auswirken, müssen durch **den Hersteller den Behörden** über eine Meldeplattform bei der **European Union Agency for Cybersecurity** (ENISA) an das „Computer Security Incident Response Team“ (CSIRT) gemeldet werden, die damit zeitgleich für die ENISA zugänglich ist.

Zum Redaktionsstand dieses Leitfadens Februar 2026 ist die Meldeplattform bei der ENISA noch nicht installiert.

Die ENISA – hat den Auftrag, ein hohes gemeinsames Niveau der Security in der EU zu fördern und zu gewährleisten und ist im Rahmen des CRA eine zentrale Melde- und Koordinationsstelle für:

- Meldungen aktiv ausgenutzter Schwachstellen
- Meldungen schwerwiegender Sicherheitsvorfälle
- Betrieb der einheitlichen Meldeplattform gemäß ↗ CRA Artikel 16.

ENISA arbeitet eng mit nationalen Behörden, CSIRTs und der Europäischen Kommission zusammen, um die digitale Resilienz Europas zu stärken.

Bei einem CSIRT handelt sich um ein spezialisiertes Team, das für die Erkennung, Analyse, Reaktion und Nachbereitung von Sicherheitsvorfällen zuständig ist.

Im CRA ist das CSIRT eine zentrale Meldestelle für:

- aktiv ausgenutzte Schwachstellen
- schwerwiegende Sicherheitsvorfälle

4 Erklärungen zum CRA des BSI: BSI – Cyber Resilience Act

In Deutschland ist das CERT-Bund[5] des Bundesamts für Sicherheit in der Informationstechnik – BSI[6] das als Koordinator benannte CSIRT.

Unter außergewöhnlichen Umständen wird das nationale Reaktionsteam für Sicherheitsvorfälle (CSIRT), das die Meldung zuerst erhalten hat, die Übermittlung der Meldung an die CSIRTs anderer EU-Länder verzögern können. Ein delegierter Rechtsakt der Europäischen Kommission mit weiteren Details für die Ausführung wurde am 11.12.2025 veröffentlicht.[7]

2.15.2 Kenntniserlangung

Die Kenntniserlangung von Schwachstellen oder Sicherheitsvorfällen ist das initiale Ereignis, das den Prozess gemäß ↗ CRA Artikel 14 in Gang setzt.

Entscheidend für die Einhaltung der Meldefristen ist der Zeitpunkt der „Kenntniserlangung“ im CRA.

DEFINITION

„Kenntnis erlangen“ im Kontext ↗ CRA Artikel 14 bedeutet, dass jemand von einem schwerwiegenden Sicherheitsvorfall oder einer bösartig ausgenutzten Schwachstelle und maßgeblichen Informationen dazu erfährt. Kenntnisnahme kann mündlich und schriftlich erfolgen.

Für die Ableitung von Aktivitäten ist es wichtig, dass die maßgeblichen Informationen zum Sachverhalt vorliegen. Auch ohne alle Detailinformationen vorliegen zu haben, muss zumindest der Kontext soweit bekannt sein, dass eine Meldung abgegeben werden kann. Im Zweifel ist es empfehlenswert eine Meldung eher unter einem vertretbaren Maß an Unsicherheit abzugeben als sie zurückzuhalten.

➔ Abbildung 11 illustriert den Prozess der Kenntniserlangung für den Hersteller des PDEs. Es wird davon ausgegangen, dass der Nutzer zuerst von dem schwerwiegenden Sicherheitsvorfall oder der aktiv ausgenutzten Schwachstelle erfährt. In der Folge informiert er den Integrator oder ggf. Hersteller einer Sub-Komponente (im Sinne des CRA sind beide Hersteller). Nun erfolgt die Analyse, um maßgebliche Informationen bereit zu haben. Gibt der Nutzer bereits detaillierte und gesicherte Informationen, so wird sofort Kenntnis erlangt, sobald der Hersteller diese Angaben verifizieren kann. Handelt es sich um eine Vermutung, muss zunächst geprüft werden, ob es sich z. B. um einen technischen Fehler oder tatsächlich um einen Security-Vorfall handelt.

Die Fristen nach ↗ CRA Artikel 14 beginnen mit dem Moment der Kenntniserlangung zu laufen. Es ist daher empfehlenswert, den Moment sowie die Quelle und die Art der erhaltenen Informationen und ggf. der durchgeführte Prozess **geeignet zu dokumentieren**.

5 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html
6 https://www.bsi.bund.de/DE/Home/home_node.html
7 Implementing regulation – EU – 2025/2392 – EN – EUR-Lex

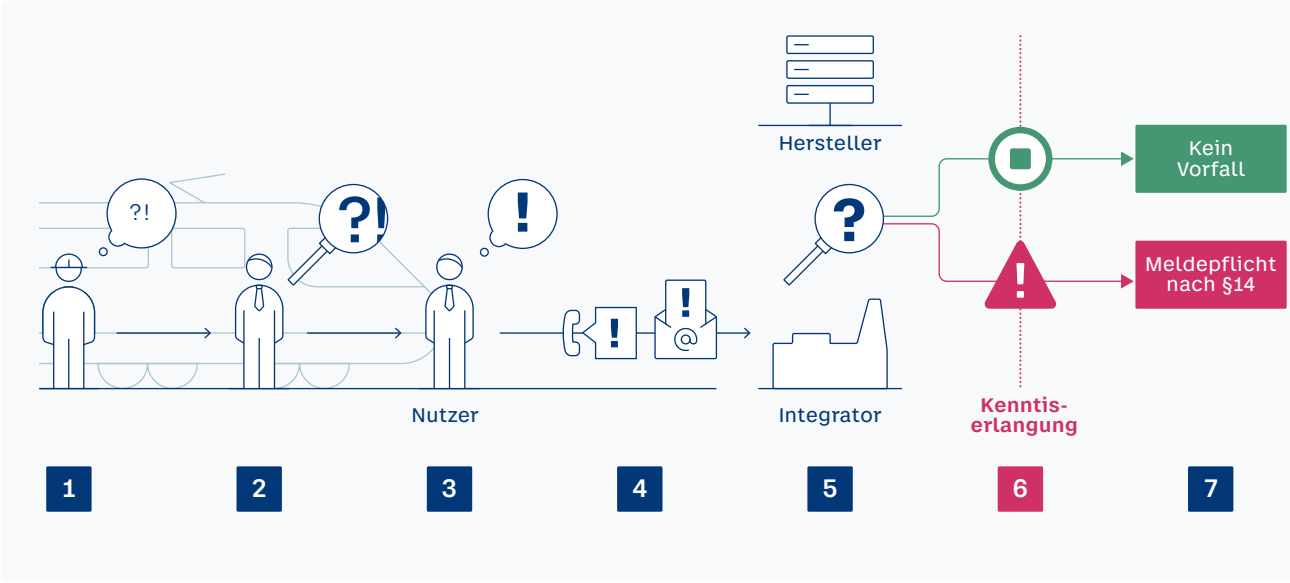

Abbildung 11: Die Kenntniserlangung

BEISPIEL

Bei Produkten im Feld würde ein Lokführer oder Werkstattmitarbeiter innerhalb seiner Organisation der Betreiber – seine Wahrnehmung „das etwas nicht stimmt“ weitergeben 1.

Der Betreiber führt eine Analyse durch 2 und kommt zu der Vermutung, dass es sich um eine ausgenutzte Schwachstelle handelt oder handeln könnte 3. Er informiert den Integrator über die vom Integrator eingerichteten Kontaktadresse (z. B. cyberalert@integrator.com) 4. Der Integrator prüft umgehend das Vorhandensein einer aktiv ausgenutzten Schwachstelle. Hierfür zieht er den Hersteller der betroffenen Komponente hinzu 5.

Hersteller und Integrator kommen zu einer Einschätzung. Dies markiert den Zeitpunkt der Kenntniserlangung 6. Ab jetzt laufen die Fristen. Liegt eine aktiv ausgenutzte Schwachstelle vor, tritt die Meldepflicht nach §14 in Kraft, liegt kein Security-Vorfall vor, ist der Vorgang beendet 7.

Integrator und Komponenten-Hersteller (beide Hersteller im Sinne des CRA) sollten beide eine Meldung abgeben.

Für den Integrator ist das PDE durch ein darin enthaltenes PDE betroffen. Er kann über die Verwendung und Verbreitung informieren.

Für den Hersteller ist das PDE direkt betroffen. Er kann über die Verbreitung des konkreten PDEs informieren.

HINWEIS

Der Betreiber würde das Ereignis auf Grundlage der NIS-2 auf dem darin beschriebenen Meldeweg ebenfalls melden (→ Kapitel 2.2.1 → Abbildung 2 „Hersteller-Nutzer-Beziehung“).

2.15.3 Meldepflichten ab 11.09.2026

DEFINITION

Alle Meldungen erfolgen an die eingerichtete einheitliche Meldeplattform ↗ CRA Artikel 16.

Die Meldepflichten gelten für alle Produkte, die der Hersteller auf dem Markt bereitgestellt hat. Das heißt, es umfasst auch bereits auf dem Markt befindliche Produkte.

Der **Hersteller meldet unverzüglich**, jedenfalls aber innerhalb von **24 Stunden**, nachdem er davon Kenntnis erlangt hat, jede aktiv ausgenutzte Schwachstelle (von Angreifern), die in dem Produkt mit digitalen Elementen enthalten ist und jeden schwerwiegenden Sicherheitsvorfall. Die Fristen gelten **nicht**:

- für potenziell ausnutzbare Schwachstellen
- für Sicherheitsvorfälle, die als nicht schwerwiegend gelten und
- nicht für die freiwilligen Meldungen gemäß ↗ CRA Artikel 15.

Der Hersteller meldet **spätestens 72 Stunden nach Kenntniserlangung** Informationen über

- Art der Ausnutzung und bereits ergriffene Maßnahmen durch Hersteller und Maßnahme, die Nutzer ergreifen können ↗ CRA Artikel 14 (2b), bzw.
- Art des Sicherheitsvorfalls, erste Bewertung und bereits ergriffene Maßnahmen durch Hersteller und Maßnahme, die Nutzer ergreifen können ↗ CRA Artikel 14 (4b).

Für die Meldefristen ist es zunächst also unerheblich, ob eine aktiv ausgenutzte Schwachstelle oder ein schwerwiegender Sicherheitsvorfall im Sinne ↗ CRA Artikel 14, (5) erkannt wurde.

Der Hersteller legt einen Abschlussbericht vor.

- Für eine ausgenutzten Schwachstelle legt der Hersteller, spätestens 14 Tage nachdem eine Korrektur- oder Risikominderungsmaßnahme zur Verfügung steht, den Abschlussbericht vor.
- Für einen schwerwiegenden Sicherheitsvorfall legt der Hersteller spätestens einen Monat nach der zweiten Meldefrist (72h) den Abschlussbericht vor.

Die ➔ Abbildung 12 illustriert die Meldefristen gemäß ↗ CRA Artikel 14.

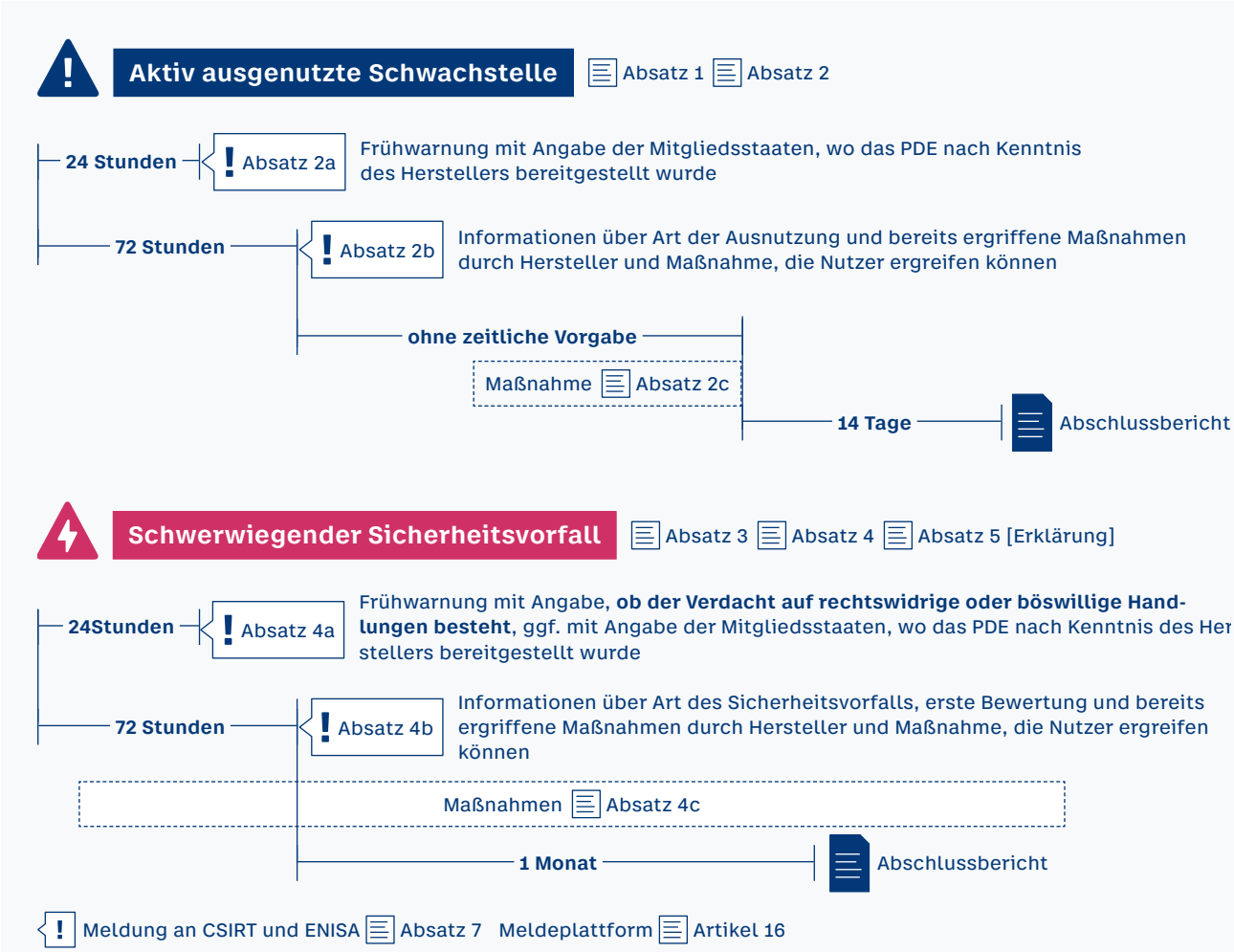

Abbildung 12: Meldepflichten der Hersteller

Der Abschlussbericht für die aktiv ausgenutzte Schwachstelle muss enthalten:

- eine Beschreibung der Schwachstelle, einschließlich ihres Schweregrads und ihrer Auswirkungen,
- falls verfügbar, Informationen über jeden böswilligen Akteur, der die Schwachstelle ausgenutzt hat oder ausnutzt,
- Informationen über die Sicherheitsaktualisierung oder andere Korrekturmaßnahmen, die zur Behebung der Schwachstelle zur Verfügung gestellt wurden.

Der Abschlussbericht für einen schwerwiegenden Sicherheitsvorfall muss enthalten:

- eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;
- Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;
- Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.

Im Fall einer **aktiv ausgenutzten Schwachstelle**, gibt es keine zeitliche Vorgabe, bis wann Korrektur- oder Risikominderungsmaßnahmen vorhanden sein müssen. In jedem Fall sind sie schnellstmöglich zu erörtern und bereitzustellen. Sobald die Maßnahme zur Behandlung bereit-

steht, verbleiben 14 Kalendertage, bis der entsprechende Abschlussbericht vorzulegen ist. Das heißt noch nicht, dass die Maßnahmen umgesetzt sind. Die Maßnahmen könnten trotzdem (wenn risikobasiert vertretbar) erst im Rahmen eines geplanten nächsten Software-Releases umgesetzt werden.

Es ist jedoch zu beachten, dass eine nicht behobene bereits einmal aktiv ausgenutzte Schwachstelle ggf. auch zu einem schwerwiegenden Sicherheitsvorfall führen kann, der dann wiederrum zu melden und wesentlich schneller zu beheben ist.

Unter der Annahme, dass für notwendige Korrekturmaßnahmen auch ein Genehmigungsverfahren (Zulassung, Typfreigabe, ...) notwendig sein kann, wird dringend empfohlen möglichst umgehend nach Erkennen des Vorfalles die Korrektur- und Risikominderungsmaßnahmen seitens der Hersteller und Korrektur- und Abhilfemaßnahmen, die Nutzer ergreifen können, einzuleiten ➔ Kapitel 3.4. Die Meldefristen für die Abschlussberichte bleiben davon unberührt.

Je nach Komplexität der Maßnahmen sind die Abschlussberichte zum Zeitpunkt der Meldung eher als ein Zwischenbericht zu verstehen, der die eingeleiteten Maßnahmen erläutert und einen Zeithorizont bis zur finalen Umsetzung und Ausrollen auf das oder die betroffenen Produkte (Systeme) aufzeigt.

Die Anforderungen gelten für **alle Produkte**, die der Hersteller auf dem Markt bereitgestellt hat. Das heißt, es umfasst auch bereits auf dem Markt befindliche Produkte, sowie wesentliche Änderungen an Produkten im Sinne von ➔ Kapitel 2.9

BEISPIEL 1

Erlangt der Hersteller Freitag 15:30 Kenntnis von einer aktiv ausgenutzten Schwachstelle, muss er

- bis spätestens Samstag, 15:30 die Meldung an die zentrale Meldeplattform geben
- bis spätestens am Montag, 15:30 die erweiterte Meldung (72h) erfolgt sein.

BEISPIEL 1

Der Hersteller wird Freitag, 22 Uhr, per Mail von einem Betreiber über eine aktiv ausgenutzte Schwachstelle im Produkt des Herstellers informiert, die beim Betreiber zu einem erheblichen Sicherheitsvorfall (NIS 2) geführt hat.

Hat der Hersteller bereits geschlossen und öffnet erst Montag, 08:00 wieder, erlangt er tatsächlich erst am Montag, 08:00 Kenntnis von der Schwachstelle. Jedoch informiert der Betreiber die zentrale Meldestelle basierend auf ↗ NIS2-UmsG § 32 (S. 24 (1) 1.) bis spätestens Samstag, 22:00 über den erheblichen Sicherheitsvorfall.

Es entstünde ein zeitlicher Versatz von mindestens 34 und maximal 58 Stunden.

HINWEIS 1

Die Meldefristen sind Zeitstunden und Kalendertage, also unabhängig von Geschäftszeiten.

HINWEIS 2

Der Hersteller sollte einen Prozess einführen, um die Meldefristen (auch außerhalb der regulären Geschäftszeiten) einhalten zu können bzw. kurzfristig reagieren zu können (24/7).

2.15.4 Meldepflichten ab 11.12.2027

Ergänzend zu ➔ Kapitel 2.15.3 gelten folgende Anforderungen ab dem 11.12.2027:

Identifiziert und dokumentiert der Hersteller **Schwachstellen auf Basis regelmäßiger und effektiver Tests**, behebt er diese entsprechend dem Risiko ohne Verzögerung und informiert die Nutzer in der Form, dass diese das Produkt und die Auswirkung identifizieren und entsprechend reagieren können.

Die Anforderungen gelten für **alle Produkte, die CRA-konform sein müssen (in Verkehr gebracht ab dem 11.12.2027)**.

2.15.5 Offenlegung von Schwachstellen (Artikel 13 und Anhang I, Teil II, Punkt 5)

Gemäß ↗ CRA Artikel 13 und Anhang I, Teil II (5) muss eine koordinierte Offenlegung von Schwachstellen erfolgen.

Im Hinblick auf Unternehmen gilt, dass die Kenntnis ihrer Mitarbeiter dem Unternehmen zugerechnet wird, das heißt wenn der Mitarbeiter Kenntnis erlangt, erlangt auch das Unternehmen Kenntnis. Daher ist seitens der Hersteller eine Strategie für die koordinierte Offenlegung von Schwachstellen aufzustellen und umzusetzen.

Das CRA beschreibt nicht wie die Offenlegung von Schwachstellen innerhalb der Lieferkette erfolgen soll.

Es ist empfehlenswert im Unternehmen einen klaren Prozess zu etablieren, der den notwendigen Informationsfluss sicherstellt. Dies muss enthalten:

- Prozess zum Absetzen der Meldung
- Prozess zur Informationsverarbeitung in der Lieferkette

HINWEIS

Das CRA spricht insbesondere im Kontext an die Anforderungen an die Behandlung von Schwachstellen im ↗ CRA Anhang I Teil II von „Veröffentlichen“. Der Begriff ist nicht definiert, es ist davon auszugehen, dass zum einen die Meldung und zum anderen die Informationen im Kreis der betroffenen Stakeholder gemeint ist. Im ersten Halbjahr 2026 wird die Veröffentlichung von Guidelines seitens der Europäischen Kommission erwartet. Hier ist eine Klarstellung zu erwarten.

3 CRA-Erfüllung im Kontext des Bahnsektors

Zuerst wird auf die einzelnen Bestandteile des Lebenszyklus eingegangen. Danach folgen Themen, welche mehrere Phasen überspannen.

3.1 Risikoanalysen

Security Risikoanalysen sind ein zentrales Instrument zur systematischen Bewertung von Bedrohungen, deren Eintrittswahrscheinlichkeit und Auswirkungen sowie der daraus resultierenden Risiken. Daraus werden geeignete Maßnahmen abgeleitet, um das Risiko zu beherrschen und auf ein zuvor definiertes, akzeptables Maß (Risikoakzeptanzniveau) abzusenken oder als Restrisiko zu dokumentieren.

Der CRA fordert gemäß CRA Artikel 13 (3) „die Bewertung des Cybersicherheitsrisikos [...] während eines [...] festzulegenden Unterstützungszeitraums“. Diese Analyse soll „dokumentiert und gegebenenfalls aktualisiert“ werden. Eine Methode für die Durchführung der Risikoanalysen wird durch den CRA nicht vorgegeben. Da sich die TS 50701 sowie die zukünftige IEC 63452 auf die Anwendung der IEC 62443 stützen, ist die Anwendung dieser zu empfehlen. Weiterhin ist die IEC 62443-4-2 in der Überarbeitung, um harmonisierter Standard nach CRA zu werden. Dies unterstützt ebenfalls die Anwendung der IEC 62443-Reihe. Grundsätzlich können auch alternative Risikomanagement-Methoden zur Anwendung gebracht werden, beispielsweise basierend auf ISO 27005. In jedem Fall ist die Anwendung eines verbreiteten Standards empfehlenswert, um die Konformität leichter argumentieren zu können.

Die Durchführung von Risikoanalysen erfolgt im Lebenszyklus wiederkehrend. Sie durchläuft verschiedene Phasen und wird im industriellen Umfeld in der Regel auf Basis der IEC 62443-3-2 durchgeführt. Die technischen Maßnahmen werden nach IEC 62443-3-3 (Systemebene) und IEC 62443-4-2 (Komponentenebene) abgeleitet und im Sinne der ganzheitlichen Betrachtung um organisatorische Maßnahmen erweitert. Die typische Abfolge ist:

1. Analyse auf Systemebene durch einen Betreiber der Anlage, z. B. Infrastrukturbetreiber
2. Übergabe der ermittelten Anforderungen (Maßnahmen) als Lastenheft
3. Pflichtenheft und Produktrisikoanalyse
   a. Überführung der Anforderungen auf Produkt (Komponenten)-Ebene durch den Integrator oder Hersteller und Nachweis zur Erfüllung der Anforderungen (Pflichtenheft)
   b. Durchführung einer produktspezifischen Risikoanalyse durch den Integrator oder Hersteller, die die vorhersehbare Betriebsumgebung berücksichtigen muss

4. Aufnahme der Risikoanalysen auf Betreiber- und Herstellerseite in die jeweilige Technische Dokumentation der PDEs
5. Wiederholung der Risikoanalysen im Lebenszyklus auf Betreiber- und Herstellerseite zyklisch (z. B. jährlich) und anlassbezogen, z. B. durch eine neue Bedrohungslage, Security-Vorfälle oder Schwachstellen

Im Bahnbereich ergänzt die TS 50701 (zukünftig IEC 63452) die IEC 62443-Reihe durch bahnspezifische Anforderungen. Die TS 50701 definiert dabei vor allem die Synchronisierungspunkte mit dem Bereich Safety und fordert die Erstellung eines Security Nachweises („Security Case“).

Sind Schritt 1 und 2 nicht verfügbar, kann der Hersteller hierzu Annahmen treffen, um die weiteren Schritte ausführen zu können.

Nachfolgend sind die wesentlichen Schritte kurz beschrieben und jeweils das Kapitel bzw. der Bereich des zugrunde liegenden Standards angegeben.

3.1.1 Definition Risikomodell

Risikoanalysen benötigen eine Grundlage zu deren Bewertung. Dies nennt man Risikomatrix. Eine Risikomatrix stellt den Zusammenhang aus Eintrittswahrscheinlichkeit (Likelihood) und Schadensausmaß (Impact) dar. Diese Werte müssen definiert werden, einheitlich Anwendung finden und im Verlauf des Lebenszyklus regelmäßig überprüft werden.

Eine Security-Risikomatrix sollte unternehmensweit gelten und mit weiteren Risikomatrizen, z. B. Safety-Risikomatrix, Business-Risikomatrix harmonisiert sein. Das heißt insbesondere, dass die möglichen Auswirkungen vereinheitlicht sind, um im Unternehmenskontext nachvollziehbare und fundierte Entscheidungen treffen zu können.

Betreiber, Hersteller und Integratoren führen separate Risikoanalysen durch, deren Abstimmung an den Schnittstellen erfolgen kann und empfohlen wird.

Die erste Achse einer Risikomatrix wird durch die potenziellen Auswirkungen (Schadensausmaß) definiert, wobei zumindest die „CIA“ Schutzziele (C-Confidentiality/Vertraulichkeit, I-Integrity/Unversehrtheit und A-Availability/Verfügbarkeit) differenziert werden müssen. Eine mögliche Differenzierung der potenziellen Auswirkungen ist in ➔ Tabelle 11 gegeben. Hier sind CIA mit spezifischeren Auswirkungen analysiert worden:

I Menschenleben
CIA Finanzielle Auswirkungen
IA Geschäftstätigkeit
CIA Gesetze
A Außenwirkung
C Privatsphäre

	Schadenskategorien und Schutzklassen			
	1 niedrig	2 mittel	3 hoch	4 sehr hoch
Menschenleben	Einzelne leicht verletzt	Einzelne schwer verletzt	Viele Verletzte, einzelne getötet	Viele können getötet werden
Finanzielle Auswirkungen (in €)	< 500.000	500.000–2 Mio.	> 10% Einnahmen oder 2–7 Mio.	> 7 Mio.
Beeinträchtigung der op erativen Geschäftstätigkeit	< 6 h	6–24 h	1–7 Tage	> 7 Tage
Verstoß gegen Gesetze/ Vorschriften	Einzelsachverhalt mit politisch/rechtlich relevanten Teilaspekten	Vertragliche, rechtliche oder politische Prüfung mit wahrscheinlichen Konsequenzen	Vertragliche, rechtliche oder politische Konsequenzen für Teile der GF/SE	Kritische vertragliche, rechtliche und politische Konsequenzen für die gesamte GF/SE
Negative Außenwirkung	Lokale Berichterstattung	Deutschlandweite und überregionale kritische Berichterstattung zu Teilbereichen/Einzelbereichen des Unternehmens	Nationale/internationale kritische Berichterstattung. Die Reputation des Konzerns ist gefährdet	Internationale Negativberichterstattung, Image des Unternehmens bei allen Stakeholdern nachhaltig beschädigt
Privatsphäre	Keine Auswirkungen (allgemein zugängliche Daten innerhalb Arbeitsverhältnis)	geringe Auswirkung	Erhebliche Auswirkung auf die Persönlichkeitsrechte der betroffenen Person oder stellt eine Straftat dar (Kunden- oder Mitarbeiterprofile)	Hohe Schutzbedürftigkeit (Verarbeitung personenbezogener Daten ist ein existenzieller Geschäftszweck)

Tabelle 11: Beispiel Definition Auswirkungen

Auf der zweiten Achse einer Risikomatrix wird die Eintrittswahrscheinlichkeit von Bedrohungen abgebildet. Um die Eintrittswahrscheinlichkeit zu definieren, gibt es keine festen Regeln aber „best practices“. Die TS 50701 schlägt die Anwendung der beiden Parameter „Exposure“ (Zugänglichkeit) und „Vulnerability“ (Verletzlichkeit) vor. Dies ist in ➔ Tabelle 12 dargestellt. Im Ergebnis mündet die Bewertung in Eintrittswahrscheinlichkeits-Kategorien, die gemeinsam mit Auswirkungs-Kategorien zur Risikoermittlung genutzt werden. Alternative Methoden zur Bestimmung der Eintrittswahrscheinlichkeit können beispielsweise der ISO 27005 und IEC 62443 entnommen werden.

Rating	Exposure (EXP)	Vulnerability (VUL)
1	**Stark eingeschränkter logischer oder physischer** Zugriff für Angreifer, z. B.: stark eingeschränkter Netzwerk- und physischer Zugriff; Produkte oder Komponenten können vom Angreifer nicht oder nur mit hohem Aufwand erworben werden	Die Schwachstelle ist nur für eine kleine Gruppe von Angreifern mit umfangreichen Hacking-Kenntnissen möglich (umfangreiche Fähigkeiten erforderlich); Die Schwachstelle kann nur mit hohem Aufwand ausgenutzt werden, dabei sind größere technische Hürden zu überwinden, zudem werden mehrfache IT-Sicherheitsmaßnahmen, um die Bedrohung entgegenzusetzen; Hohe Wahrscheinlichkeit, dass Angreifer aufgespürt und schadlos erfolglos wird
2	**Eingeschränkter logischer oder physischer Zugriff** für Angreifer, z. B.: interner Netzwerkzugriff erforderlich oder eingeschränkter physischer Zugriff oder Produkte oder Komponenten können vom Angreifer nicht oder nur mit hohem Aufwand erworben werden	Ein erfolgloser Angriff ist nur für einen Angreifer mit durchschnittlichen Hacking-Kenntnissen möglich (mittlere Fähigkeiten erforderlich); Die Schwachstelle kann mit mittlerem Aufwand ausgenutzt werden, erfordert spezielle Technologie-, Domänen- oder Tool-Kenntnisse; Einige IT-Sicherheitsmaßnahmen, um der Bedrohung entgegenzuwirken; Mittlere Wahrscheinlichkeit, dass Angreifer aufgespürt und schadlos erfolglos wird
3	**Einfacherer logischer oder physischer Zugriff** für Angreifer, z. B.: Internetzugriff ausreichend oder öffentlicher physischer Zugriff oder der Angreifer hat im Rahmen der täglichen Arbeit, des Betriebs oder der Instandhaltung Zugriff oder Produkte oder Komponenten können vom Angreifer mit geringem Aufwand erworben werden	Ein erfolgreicher Angriff ist selbst für einen ungelernten Angreifer einfach durchzuführen (nur geringe Fähigkeiten erforderlich); Die Schwachstelle kann mit geringem Aufwand ausgenutzt werden, es müssen keine Tools benötigt werden oder die geeigneten Angriffs-Tools frei erhältlich sind; Keine oder nur schwache IT-Sicherheitsmaßnahmen, um durch die Sicherung verursachten Angriff entgegenzusetzen; Geringe Wahrscheinlichkeit, dass Angreifer aufgespürt und schadlos erfolglos wird

Tabelle 12: Beispiel Bestimmung Eintrittswahrscheinlichkeit TS 50701

Nach dem Beispiel der TS 50701 ermittelt sich die Eintrittswahrscheinlichkeit aus (Exp+Vul)-1.

Die Kombination der potenziellen Auswirkungen und Eintrittswahrscheinlichkeiten ergibt die Risiken. Die Risiken werden üblicherweise in vier bis fünf Risikokategorien eingestuft, wobei ein Risikoakzeptanzniveau für nachfolgende Prozesse (z. B. Restrisikodeklaration) zwingend zu definieren ist. Möglich ist auch eine zweistufige Festlegung auf „maximal akzeptables Risikoniveau“ und „Ziel-Risikoniveau“. Häufig ist das Ziel-Risiko-Niveau „Gering“ und das maximal akzeptable Risiko „Mittel“. Ein Beispiel ist in ➔ Tabelle 13 zu sehen.

Eintrittswahrscheinlichkeit	Impact 1	2	3	4	5
1	gering	gering	gering	gering	gering
2	gering	gering	gering	mittel	mittel
3	gering	gering	mittel	mittel	hoch
4	gering	mittel	mittel	hoch	extrem
5	gering	mittel	hoch	extrem	extrem

Tabelle 13: Beispiel Risikomatrix

Zusätzlich ist für die Durchführung der Risikoanalyse ein Bedrohungsmodell notwendig. Best Practice ist, Bedrohungen und die dazugehörigen Sicherheitslücken ganzheitlich zu identi-

fizieren. Dazu gehören z. B. erwartbare Software-Schwachstellen, fehlkonfigurierte Hosts, organisatorische Mängel oder Probleme mit der physikalischen Infrastruktur. Bei diesem Prozess sind zudem etablierte Kataloge, Modellierungsansätze und Datenbanken zu berücksichtigen. Beispiele sind:

- MITRE ATT&CK ICS Matrix[8]
- VATT&EK Rail Vehicle Attack Matrix[9]
- BSI Katalog Elementare Gefährdungen[10]
- STRIDE

3.1.2 Systemdefinition und Kontextanalyse

Sind die Grundlagen für das Risikomanagement gelegt, kann der Prozess zur Risikobewertung gestartet werden. Er beginnt mit der Definition des Betrachtungsumfangs, der gemäß Best Practice das eigene PDE, direkte Kommunikationspartner und die Betriebsumgebung beinhalten muss. Das PDE muss mit seinen Schnittstellen, wesentlichen Funktionen und der vorhersehbaren Verwendung betrachtet werden. Diese ganzheitliche Betrachtung ist essenziell für die im CRA geforderte Bewertung der „Ausnutzbarkeit von Schwachstellen“ (➔ Kapitel 3.2), die wesentlich von der Erreichbarkeit für Angreifer abhängt.

Zum Beispiel ein Feld-Element-Controller für eine Weiche mit den Schnittstellen Safety-Kommunikation, Software-Update, Diagnose-Daten und Security-Services. Ein anderes, komplexeres Beispiel wäre das vollständige Stellwerk inklusive seiner Außenelemente.

Dieser Arbeitsschritt entspricht ZCR-1 nach IEC 62443-3-2.

3.1.3 Initiale Risikoanalyse

Im nächsten Schritt erfolgt die initiale Risikobewertung. In diesem Schritt wird auf Basis der in ➔ Kapitel 3.3.1 dargestellten Auswirkungskategorien die Kritikalität von Komponenten bewertet. Dabei ist die Zweckbestimmung der Komponenten entscheidend.

Bei Anwendung der IEC 62443-3-2, entspricht dieser Arbeitsschritt ZCS-2 und ZCS-3. Er ermöglicht die Darstellung von Zonen und Conduits.

Eine Zone gibt einen Bereich gleicher Kritikalität an einem Ort an. Das heißt z. B. die Zusammenfassung des Stellwerks-Kerns mit einem Notbedienplatz wäre denkbar. Die Manipulation kann jeweils katastrophale Auswirkungen haben.

Ein Conduit beschreibt die Verbindung zwischen zwei Zonen. Das Conduit erlaubt die Kontextualisierung und Zuordnung von Maßnahmen an Zonenrändern, z. B. Verschlüsselung am Übergang Zone zu Conduit.

8 https://attack.mitre.org/
9 https://vehicle-threat-matrix.com/node/152
10 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare_gefaehrdungen.html

Für Zonen werden im nächsten Schritt detaillierte Risikoanalysen durchgeführt. Für Conduits werden keine detaillierten Risikoanalysen durchgeführt. Sie gelten aus Security-Sicht als transparente, unsichere Kanäle. Soll ein Conduit behandelt und geschützt (secure) werden, so wird er wieder als Zone betrachtet.

Wichtig: Die initialen Risikoanalysen sind ohne Security-Maßnahmen aber unter Berücksichtigung von Umgebungsbedingungen (Gebäude, Gebäude-Schutz, örtliche Lage, Anwendungsbereich, ...) durchzuführen. Nur so wird sichergestellt, dass das richtige Security-Level (SL) definiert und die richtigen Anforderungen gestellt werden können. Würde man Security-Maßnahmen als gegeben annehmen, so blieben Risiken undefiniert oder unbehandelt. In der Folge kann es zu schwerwiegenden Versäumnissen im Prozess des Anforderungsmanagement und der Entwicklung kommen.

3.1.4 Detaillierte Risikobewertung

In der detaillierten Risikoanalyse werden auf Basis der Kritikalität von Komponenten des in → Kapitel 3.3.1 definierten Risikomodells die Risiken detailliert bewertet und iterativ Gegenmaßnahmen zur Risikominderung definiert, bis das Akzeptanzniveau erreicht ist oder verbleibende Risiken als Restrisiken dokumentiert werden müssen.

Bei Anwendung der IEC 62443-3-2 entspricht dieser Arbeitsschritt ZCR-5. Kurz zusammengefasst wird je Zone:

1. Die Auswirkung jeder Bedrohung (und ggf. Sicherheitslücke[11] im System) bewertet. Dazu werden Eintrittswahrscheinlichkeit, potenzielle Auswirkung und daraus das Risiko ermittelt.
2. Es wird das ungeminderte Risiko ermittelt und mit dem Zielrisiko verglichen.
3. Es werden (wenn das Zielrisiko nicht erreicht ist) risikomindernde Maßnahmen, wie z. B. aus IEC 62443-3-3 auf Systemebene oder IEC 62443-4-2 auf Komponentenebene, ausgewählt.
4. Die Prozessschritte 1-3 werden so lange wiederholt, bis das Zielrisiko erreicht ist oder es keine vernünftige Maßnahme zur Beherrschung mehr gibt.
5. Das Ergebnis wird dokumentiert.

3.1.5 Maßnahmendefinition

Für Hersteller ist es erforderlich, für die ausgewählten Maßnahmen eine detaillierte Spezifikation zu erstellen. Integratoren stellen damit die Passfähigkeit in ihr Gesamtsystem sicher. Komponenten-Hersteller stellen damit die Grundlage ihrer Entwicklung sicher (Pflichtenheft).

Einige praktische Beispiele können sein:

11 Achtung: Die Sicherheitslücke ist nicht auf Software-Schwachstellen (Verwundbarkeiten, engl. „*vulnerabilities*“) begrenzt. Auch die Fehlkonfiguration einer Komponente, eine leicht zugängliche physikalische Schnittstelle oder ein schwacher physikalischer Schutz kritischer Komponenten können Sicherheitslücken sein.

1. Definition des Zertifikatsmanagementprotokolls, um die PKI standardisiert nutzen zu können, z. B. CRL über CMP nach RFC 9483
2. Definition des Verschlüsselungsalgorithmus, um Kommunikation zwischen verschiedenen Systemen nativ zu erlauben, z. B. TLS 1.3 mit Elliptic Curves nach BSI-Empfehlung
3. Definition des Zeitprotokolls, z. B. NTS nach RFC 8915

Bei Anwendung der IEC 62443-3-2 basieren die ausgewählten Maßnahmen auf der IEC 62443-3-3 oder 4-2. Betreiber sind angehalten, eine Detaillierung auf IEC 62443-3-3 Level vorzunehmen, wenn dies für die Interoperabilität in ihrem eigenen Betrieb erforderlich ist.

3.1.6 Dokumentation und Monitoring

Risikoanalysen sind regelmäßig zu wiederholen. Die Wiederholung wird durch zwei Mechanismen angestoßen:

1. Zeit-induziert: Regelmäßige Überprüfung nach festen Zyklen, z. B. jährlich
2. Ereignis-induziert: Wiederholung nach Sicherheitsvorfall, Änderung der Bedrohungslage, etc.

Die Änderung der Bedrohungslage inkludiert, dass für den Software-Stack des PDEs neue Schwachstellen identifiziert wurden. Hier muss über die Security Risikoanalyse die „Ausnutzbarkeit“ ermittelt und anhand der Kritikalität die Priorität möglicher Gegenmaßnahmen festgelegt werden.

3.2 Schwachstellen Management und Security-Updates

3.2.1 Definitionen

Gemäß CRA sollen Hersteller von Produkten mit digitalen Elementen (PDE) unverzüglich Maßnahmen zur Behebung erkannter Schwachstellen ↗ CRA Artikel 13 (6) einleiten. Um diese Anforderung erfüllen zu können, sind mehrere Prozesse zu etablieren und Zeiträume zu beachten. Diese sind folgend je kurz definiert und erläutert:

Unterstützungszeitraum: Hersteller müssen einen Unterstützungszeitraum festlegen, der sich nach der voraussichtlichen Nutzungsdauer des Produkts richtet. Die Mindestdauer für den Support beträgt fünf Jahre bzw. der erwarteten Nutzungsdauer des PDEs. Der Zeitraum kann je nach PDE auch über- oder unterschritten werden. Während dieses Zeitraums müssen Security Updates bereitgestellt und Schwachstellen effektiv behandelt werden (↗ CRA Artikel 13 (8)).

Cybersicherheitsanforderungen: Hersteller müssen während des gesamten Unterstützungszeitraums alle „grundlegenden Cybersicherheitsanforderungen“ erfüllen. Dazu gehören ins-

besondere das Schwachstellen Management und regelmäßige Security Risikoanalysen. Sind bestimmte „grundlegende Cybersicherheitsanforderungen“ auf ein Produkt mit digitalen Elementen nicht anwendbar, sollte der Hersteller dies in der Security Risikoanalyse eindeutig begründen ↗ CRA Artikel 13 (3) und (4)).

Automatische Updates: Produkte mit digitalen Elementen können automatische Funktionen zur Benachrichtigung, zur Verteilung, zum Herunterladen und zur Installation von Security Updates bieten. Im Anwendungsgebiet der betriebsrelevanten Produkte für Bahnen sind automatische Updates nicht zu erwarten.

Schwachstellen identifizieren: Es sollen Prozesse zur Identifikation und Bewertung von Schwachstellen etabliert werden. Dazu zählen:

- Schwachstellenmeldungen interner und externer Quellen ↗ CRA Artikel 13 (10) auswerten inklusive Bereitstellung Meldeweg für erkannte Schwachstellen ↗ CRA Anhang I Teil II (6)
- **Regelmäßige Tests** und Überprüfung der PDEs hinsichtlich Schwachstellen ↗ CRA Anhang I Teil II (3)
- Strategie zur koordinierten Offenlegung ↗ CRA Anhang I Teil II (5), ➔ Kapitel 2.15.5

Security Maßnahmen: Nach der Identifikation und Bewertung von Sicherheitslücken (unter anderem Schwachstellen), sollen Maßnahmen zur Bewältigung bereitgestellt werden. Die Mitigation kann durch die Bereitstellung von Security Updates oder durch kompensierende Maßnahmen erfolgen. Die Effektivität der ausgewählten Maßnahmen ist über die Security Risikoanalysen (➔ Kapitel 3.1) zu bewerten.

Systeme und Produkte müssen fähig sein, Security Updates zu erhalten, um auftretende Schwachstellen zu beheben. Dies wird durch die Anwendung der Security im Entwurf (Security by design) ermöglicht ↗ CRA Anhang I Teil I (2k).

Dokumentation und Offenlegung von Schwachstellen: Hersteller sollen eine Strategie haben, um Schwachstellen zu behandeln. Sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, muss der Hersteller die Nutzer informieren. Dies schließt auch eine klare Dokumentation und die Benachrichtigung über Security Updates eint ↗ CRA Anhang I Teil II (4) und (5).

Der Zugriff auf die Informationen soll für die Nutzer leicht sein. Sind alle Nutzer bekannt, kann eine aktive Information möglich sein. Sind nicht alle Nutzer bekannt, bietet sich eine Plattform zur Information über Security Updates an.

Unabhängigkeit: Software Updates (Feature-Drop) sollen nach Möglichkeit unabhängig von Security Updates ausgerollt werden ↗ CRA Anhang I Teil II (2). Für betriebsrelevante Produkte im Bahnbereich ist dies unbedingt erforderlich, um Re-zertifizierungen bei Anwendung von Security Updates zu vermeiden.

Auslieferung ohne bekannte ausnutzbare Schwachstellen: Als „ausnutzbare Schwachstelle“ gilt eine Schwachstelle, die von einem unbefugten Dritten unter praktischen Betriebsbedingungen wirksam genutzt werden kann. Die Bewertung der Ausnutzbarkeit basiert auf der Security Risikoanalyse (➔ Kapitel 3.1).

HINWEIS

Gemäß Produkthaftungsrichtlinie (EU) 2024/2853 gelten Produkte ohne ausreichende Cybersicherheit als fehlerhaft. Dies gilt auch bei fehlenden Updates oder Upgrades zur Behebung von Schwachstellen (Erwägungsgrund 51, (EU) 2024/2853). Die Produkthaftungsrichtlinie ist im Dezember 2024 in Kraft getreten und muss bis Dezember 2026 in nationales Recht überführt werden. Anschließend folgt keine weitere Übergangsfrist.

Security Updates und Software Updates: Es wird zwischen Security und Software Updates unterschieden.

Bei Software Updates im Generellen handelt es sich um Updates, die unter anderem auch Security Updates enthalten können, aber im Wesentlichen für die Implementation von neuen Features oder Änderungen an der Verhaltensweise eines Produktes gedacht sind.

Bei Security Updates handelt es sich um Updates, deren Zweck es ist, bestehende Schwachstellen des Produktes zu beheben oder zu behandeln. Dabei werden im Regelfall weder neue Features in das Produkt eingebracht, noch ändert sich üblicherweise die Verhaltensweise des Produktes.

In der nachfolgenden ➔ Tabelle 14 sind die Unterschiede übersichtlich zusammengefasst.

Kriterium	Software Update	Security Update
Zweck	Verbesserung, Erweiterung oder Änderung von Funktionen	Schließen von Schwachstellen, Behebung von Sicherheitslücken
Beispiele	Neue Features, Performance-Optimierung, UI-Verbesserung, Stabilitätsupdate	Patch gegen Zero-Day-Lücken, Updates zur Härtung gegen Angriffe, Bugfixes mit Sicherheitsrelevanz
Fokus	Mehrwert, Benutzerfreundlichkeit, Funktionalität	Schutz von Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit
CRA-Relevanz	Nicht verpflichtend, aber möglich	Verpflichtend – Hersteller müssen Security Updates über den gesamten Produktlebenszyklus bereitstellen

Tabelle 14: Software und Security Updates

3.2.2 Anwendung

Das Management von Änderungen für ein PDE stützt sich auf ein etabliertes Asset- und Konfigurationsmanagement. Dazu gehört die Übersicht:

- aller verbauten Komponenten,
- Software, Firmware und
- bestehende Patches.

Industriestandards enthalten nützliche Informationen und Leitlinien:

- **IEC/TR 62443-2-3:2015** enthält detaillierte Informationen zur Umsetzung von Security Updates in einer IACS-Umgebung.
- Das Management von Security Updates von Bahnsystemen unter Gewährleistung von betrieblichen Anforderungen wird in **CLC TS 50701:2023**, Kapitel 10.3.2, beschrieben.
- Darauf aufbauend beschreibt die **DIN VDE V 0831-105** einen risikobasierten Ansatz zur Bewertung und Behandlung von Sicherheitslücken und -vorfällen bei Produkten und Systemen der Eisenbahnautomatisierung.

Vertiefende Beispiele für die Risikobewertung können ➔ Kapitel 3.1 entnommen werden.

Für die Kategorisierung von Security Updates schlägt DIN VDE V 0831-105 vier Kategorien vor. Diese sollen dabei helfen zu klassifizieren, wie dringend die Änderung umzusetzen ist und welcher zeitliche Aufwand damit verbunden ist.

DEFINITION

Kategorie 1 | Regelmäßige Änderungen: Diese sind im Security Case schon vorgesehen und es gibt einen vorab definierten Prozess zu ihrer Einbringung, z. B. planmäßige Updates von Virus-Signaturen. Diese sind keine Schwachstellen und damit außerhalb des Anwendungsbereichs des Schwachstellen-Managements.

Kategorie 2 | Geringfügige Änderungen: Weder der Security Case noch der Sicherheitsnachweis (Safety Case) müssen angepasst werden, z. B. einfache Bug Fixes – das heißt der Security Case war korrekt, aber die Implementierung nicht.

Kategorie 3 | Änderungen in der Security: Der Security Case muss angepasst werden, aber die Schnittstelle zur Safety ändert sich nicht, das heißt der Sicherheitsnachweis (Safety Case) bleibt bestehen. Z. B. könnte der Security Case fehlerhaft sein oder die Security Funktionalität hat sich geändert.

Kategorie 4 | Änderungen mit Auswirkung auf die Safety: Der Security Case ändert sich, und auch die Schnittstellen zur Safety, z. B. Latenzzeiten.

Gemäß dieser Definition ist eine geplante Änderung in der Security (**Kategorie 1**) nicht Gegenstand der Anforderungen des CRA, da diese nicht auf eine Schwachstelle zurückzuführen ist.

Eine Sicherheitsaktualisierung nach CRA kann als geringfügige Änderung (**Kategorie 2**) betrachtet werden, insofern ein Nachweis der Rückwirkungsfreiheit auf die Produktfunktionen

und geltende Anwendungsbedingungen geführt werden kann. Dann kann die Schwachstelle über ein Security Update behoben werden.

Eine Änderung ohne Auswirkung auf die Safety, aber mit Auswirkung auf die Security Strategie **(Kategorie 3)**, führt zu einem höheren Aufwand, da der Security Case angepasst werden muss. Technisch lässt sich diese Maßnahme jedoch zügig umsetzen, da keine Safety-bezogenen Anpassungen erfolgen müssen. Änderung mit Auswirkungen auf die Safety (**Kategorie 4**) lassen sich nicht ohne weiteres auf Sicherheitsaktualisierungen gemäß CRA abbilden und sind dem regulären Software-Änderungs-Prozess zuzuordnen. Heutige Produkte mit digitalen Elementen fallen häufig unter Kategorie 4. Das Ziel der Produktentwicklung muss nach CRA sein, Produkte so zu entwickeln, dass sie Security Updates „einfach“ erhalten können ↗ CRA Anhang I Teil I (2k). Neben dem CRA bietet dies auch strategische Vorteile für Obsoleszenz Management und gemeinsame Nutzung von Plattformen.

3.3 Produktlebenszyklen

Grundsätzlich ist der CRA für alle Phasen im Lebenszyklus eines PDEs, von der Entwicklung bis zum Ende der Nutzung, relevant. Die Relevanz ergibt sich dabei nicht nur aus den Verpflichtungen, die der CRA den unterschiedlichen Rollen auferlegt, sondern auch aus den daraus entstehenden Konsequenzen. Die Phasen des Lebenszyklus eines PDEs können sich auch überlappen, wobei die Überlappung je nach PDE unterschiedlich ausgeprägt sein kann. So kann die Phase des Vertriebs für PDEs, die spezielle Anforderungen hat, bereits vor der Produktentwicklung beginnen, für PDEs, die für einen allgemeinen Markt bestimmt sind, aber auch erst bei der Produktion starten. Die nachfolgende ➔ Abbildung 13 stellt dabei alle möglichen Überlappungen dar und ist in diesem Sinne nicht als allgemeingültig zu verstehen. Sie bezieht sich nur auf neue PDEs und nicht auf solche, die bereits auf dem Markt bereitgestellt wurden. ➔ Abbildung 13 zeigt eine beispielhafte Darstellung der verschiedenen Lebenszyklusphasen.[12]

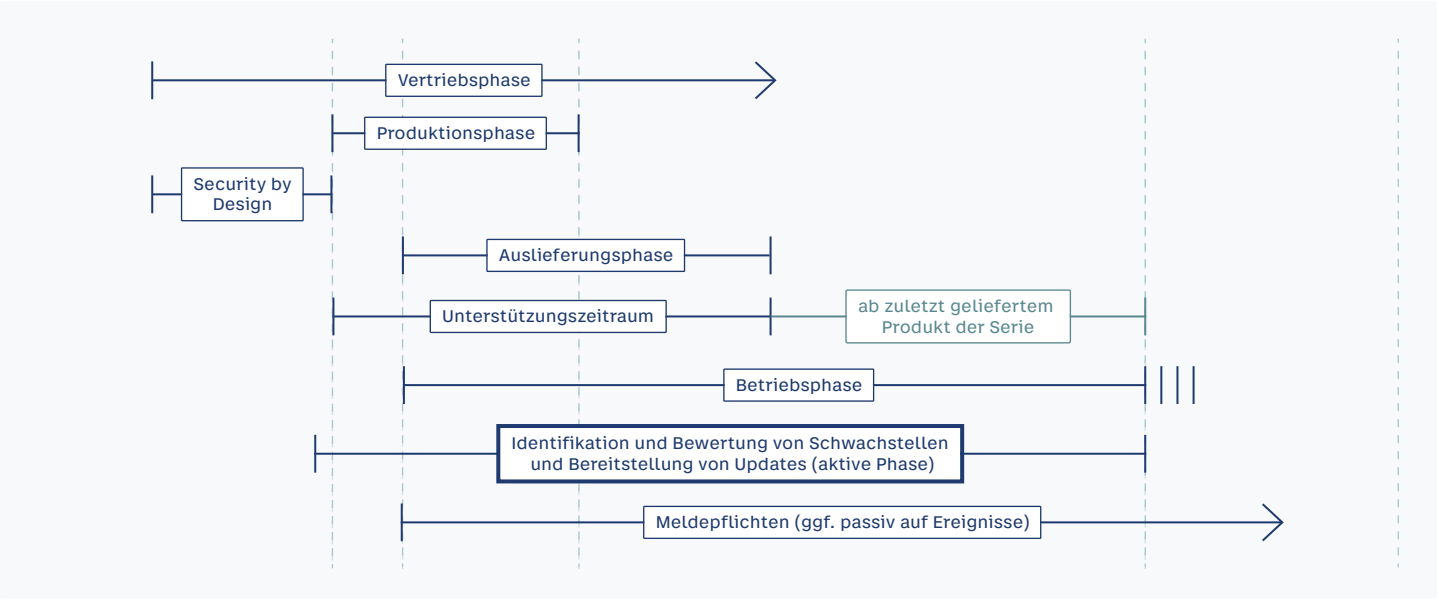

Abbildung 13: Produktlebenszyklen

12 x und y sind je nach PDE individuelle Zeitintervalle.

3.3.1 Vertriebsphase

Die Vertriebsphase eines PDEs kann je nach PDE zu verschiedenen Zeitpunkten beginnen oder enden. Es ist möglich, dass der Vertrieb schon vor der Entwicklung eines PDEs beginnt und erst deutlich nach der Produktion endet. Dies ist zum Beispiel bei maßgeschneiderten PDEs der Fall, wenn das PDE erst auf die Anforderung des Nutzers (vergleiche Definition Nutzer und Kunde in ➔ Kapitel 2.2.1 hin entwickelt wird. Wird das PDE nach der Herstellung und Auslieferung weiterhin auch anderen Nutzern angeboten, kann sich die Vertriebsphase über die Produktionsphase hinaus erstrecken, wenn nach Ende der Produktion noch Lagerbestände verkauft werden.

Aus Sicht des CRAs spielt der genaue Zeitraum des Vertriebs eigentlich keine Rolle. Entscheidend ist hier eher, dass in der Vertriebsphase bereits eine Bereitstellung auf dem Markt entstehen kann, wodurch einige Herstellerverpflichtungen greifen. Dies gilt auch, wenn das PDE noch nicht ausgeliefert ist. Dies ist zum Beispiel dann der Fall, wenn bereits ein geschlossener Vertrag über die Abgabe eines hergestellten PDEs besteht, dieses aber noch nicht ausgeliefert wurde.

Zum Zeitpunkt der erstmaligen Bereitstellung des PDEs auf dem EU-Markt werden nachfolgende Anforderungen aus dem CRA relevant:

- Das PDE darf über keine bekannten und ausnutzbaren Schwachstellen verfügen.
- Das PDE muss mit einer sicheren Standardkonfiguration bereitgestellt werden.
- Die vorgeschriebene technische Dokumentation muss vorhanden sein.
- Risikobewertung für das PDE muss in der technischen Dokumentation vorhanden sein.

3.3.2 Design- und Entwicklungsphase

Die Vorgaben des CRA beginnen bereits in der Entwicklungsphase eines PDEs mit digitalen Elementen zu greifen. An dieser Stelle ist ausschließlich der Hersteller vom CRA betroffen. Sie müssen im Einklang mit dem CRA die folgenden Punkte bei der Entwicklung eines PDEs berücksichtigen:

- Bei der Integration von zugekauften PDEs sollte geprüft werden, ob diese über eine CE-Kennzeichnung verfügen und bekannte Schwachstellen vorliegen. Um Schwachstelleninformationen zu erhalten, kann auf Einträge in den CVE-Datenbanken zurückgegriffen werden.
- Der Hersteller der Zukaufprodukte sollte den aktuellen Stand hinsichtlich Schwachstellen dem Empfänger/Nutzer mitteilen.
- Soweit möglich und leistbar kann der Empfänger/Nutzer der Zukaufprodukte den Stand eigenständig aktuell halten.
- PDEs sollen mit einer sicheren Standardkonfiguration auf den Markt gebracht werden. Dies muss bei der Entwicklung eines neuen PDEs bereits berücksichtigt werden.
- Für Software schreibt der CRA die Erstellung einer Softwarestückliste (SBOM) vor, die dem Hersteller helfen soll Schwachstellen in zugelieferter Software zu erkennen. Hier empfiehlt es sich die SBOM direkt bei der Entwicklung eines PDEs automatisiert zu erstellen und aktuell zu halten, da eine nachträgliche Ermittlung der verwendeten Software oft aufwendiger ist, als diese direkt zu dokumentieren. Zudem sollten Hersteller

überlegen, eine ähnliche Liste für zugekaufte Komponenten zu erstellen, da auch hier eine nachträgliche Ermittlung oft langwieriger ist.

- Hersteller müssen gemäß ↗ CRA Artikel 13 (8) den Unterstützungszeitraum ihres PDEs so festlegen, dass er der voraussichtlichen Nutzungsdauer des PDEs entspricht. Es empfiehlt sich den Unterstützungszeitraum bereits während der Produktentwicklung festzulegen. Hierdurch kann beim Zukauf von Komponenten berücksichtigt werden, dass sie nach Möglichkeit ähnliche Unterstützungszeiträume bieten. Es ist dabei zu beachten, dass der Unterstützungszeitraum immer für ein einzelnes PDE gilt. Dies hat zur Folge, dass die Pflicht zur Unterstützung mit Bereitstellung des ersten PDEs beginnt, der Unterstützungszeitraum jedoch erst mit der letzten Bereitstellung des PDEs dieser Serie beginnt abzulaufen. Wird zum Beispiel ein Unterstützungszeitraum von fünf Jahren für ein Handy festgelegt, so endet die Verpflichtung des Herstellers erst fünf Jahre nach der Bereitstellung des letzten Handys dieser Serie.
- Für jedes PDE ist laut CRA eine geeignete technische Dokumentation bereitzustellen, die unter anderem die Konformitätserklärung beinhaltet. Diese sollte am Ende der Entwicklungsphase vorhanden sein.

Laut CRA muss bei der Entwicklung eines PDEs der Ansatz „Secure by Design“ berücksichtig werden. Dies bedeutet, dass bei der Entwicklung (Secure Development) aktuellen Regeln der Technik oder Industriestandards (z. B. gemäß IEC 62443) gefolgt wird, auf mögliche Schwachstellen geachtet wird und die Auswirkungen eines möglichen Sicherheitsvorfalls durch produktinterne Barrieren und Abgrenzungen auf ein Minimum reduziert sein sollten.

3.3.2.1 Secure by design

„Secure by Design“ beschreibt einen sicherheitsorientierten Entwicklungsansatz, bei dem Cybersicherheitsmaßnahmen von Beginn an – also bereits in der Planungs- und Entwurfsphase – systematisch berücksichtigt und in das Gesamtsystem integriert werden. Ziel ist es, potenzielle Schwachstellen frühzeitig zu identifizieren und zu beheben, bevor ein System in Betrieb genommen wird.

Es ist essenziell, dass Sicherheitsaspekte nicht nachträglich ergänzt, sondern als integraler Bestandteil des Systemdesigns verstanden und umgesetzt werden. Hierzu sollten folgende Grundprinzipien umgesetzt werden:

- **Frühzeitige Sicherheitsanforderungen:** Security Ziele werden bereits in der Konzeptionsphase definiert.
- **Minimierung der Angriffsfläche:** Systeme werden so gestaltet, dass potenzielle Angriffspunkte reduziert werden.
- **Mehrschichtige Sicherheitsarchitektur (Defense in Depth):** Kombination verschiedener Schutzmechanismen zur Erhöhung der Resilienz.
- **Sichere Standardkonfigurationen:** Systeme sind im Auslieferungszustand sicher konfiguriert.
- **Verantwortungskaskade:** Umsetzung von Verantwortlichkeit für Cyber Security setzt eine definierte Verantwortungskaskade voraus (➔ Kapitel 2.2).

Weitere Informationen zum Thema „Secure by Design“ können ↗ CRA Anhang I und der einschlägigen Fachliteratur entnommen werden.

3.3.2.2 Erstellung einer SBOM (Software Bill of Material)

Bei einer Software-Stückliste (Software Bill of Materials, SBOM) handelt es sich um ein formelles, maschinenlesbares Inventar, welches die Komplexität von Software in einem PDE transparent repräsentiert. Sie enthält Informationen über alle in der Software genutzten Bestandteile und Abhängigkeiten wie deren Hersteller, Version, Lizenzinformation und weitere Angaben. Diese Bestandteile können beispielsweise Anwendungen, Betriebssysteme, Firmware, Libraries oder Services sein.

Um den CRA einzuhalten, ist jeder Hersteller bzw. Integrator für die Erstellung und Analyse „seiner" SBOM verantwortlich und muss sofern nicht anders vereinbart die SBOMs der Zulieferer nicht kennen und analysieren. Aus Produktsorgfaltspflicht kann dies dennoch in Betracht gezogen werden.

In einem System, z. B. Zug oder Stellwerk, gibt es unterschiedliche SBOMs, die den jeweiligen PDEs zugeordnet sind, z. B. Komponenten, Teilsysteme oder Systeme.

SBOMs werden in der Branche häufig eingesetzt, um die Transparenz zu erhöhen und als essenzieller Teil für das Schwachstellen Management die Identifizierung von Schwachstellen zu beschleunigen. Sie können kontinuierlich mit einer Schwachstellendatenbank wie CVE (Common Vulnerabilities and Exposures)[13] oder European Vulnerability Database (EUVD)[14] abgeglichen werden.

Für die Erstellung einer SBOM fordert der CRA ein maschinenlesbares Format. Das BSI stellt mit „TR-03183: Cyber Resilience Requirements for Manufacturers and Products – Part 2: Software Bill of Materials (SBOM)"[15] eine technische Guideline zur Verfügung. Dort benennt das BSI die Formate CycloneDX und Software Package Data eXchange (SPDX).

Als Hilfestellung für die Erstellung von mit TR-03183-Teil 2 konformen SBOMs hat das BSI einen eigenen CycloneDX Namensraum angelegt und diesen bei CycloneDX registriert. Dessen Taxonomie ist innerhalb des BSI-GitHub-Account[16] veröffentlicht.

Um die SBOMs für jede Software-Version aktuell zu halten, wird empfohlen die Erstellung in die Software-Entwicklungspipeline zu integrieren und automatisch zu generieren.

3.3.3 Produktionsphase

Der CRA schreibt in ↗ CRA Anhang I vor, dass ein PDE ohne bekannte Schwachstellen und mit einer sicheren Konfiguration auf dem Markt bereitgestellt werden muss. In der Konsequenz muss diese Anforderung bereits bei der Herstellung von PDEs berücksichtigt werden.

So kann es zum Beispiel passieren, dass während der Produktionsphase Schwachstellen im PDE selbst entdeckt werden. Dies hat zur Folge, dass die Schwachstelle entsprechend behandelt werden muss. Die Art der Behandlung ist fallspezifisch. Ist hier nicht vorgesorgt worden, können hohe Aufwände und damit verbunden auch hohe Kosten entstehen. Es ist

13 https://nvd.nist.gov/vuln/search#/nvd/home
14 https://euvd.enisa.europa.eu/
15 https://bsi.bund.de/dok/TR-03183
16 https://github.com/BSI-Bund/tr-03183-cyclonedx-property-taxonomy

daher empfehlenswert, den Produktionsprozess derartig zu entwerfen, dass Softwareversionen und Konfigurationsdateien einfach ausgetauscht werden können. Zudem sollte die Lagerhaltung von Komponenten so geplant werden, dass der Wechsel auf eine neue Version schnell vonstattengehen kann.

3.3.4 Inverkehrbringen und Auslieferungsphase

Gemäß ➔ Kapitel 2.4 wird ein PDE in den Verkehr gebracht, wenn es zum ersten Mal auf dem Unionsmarkt bereitgestellt wird. Nach der Herstellung und dem Vertrieb eines PDEs kann es nun ausgeliefert werden. Spätestens hier muss von einer Bereitstellung auf dem europäischen Markt ausgegangen werden, wodurch die in der Vertriebsphase beschriebenen Anforderungen relevant werden. Zudem beginnt spätestens mit der Auslieferung eines jeden PDEs der Unterstützungszeitraum, in dem Schwachstellen identifiziert und durch Updates oder andere Maßnahmen behoben werden müssen.

3.3.5 Betriebsphase

Mit Betriebsphase ist hier der Zeitraum gemeint, in dem ein PDE tatsächlich durch den Nutzer betrieben wird. Für diesen Zeitraum macht der CRA keine direkten Vorgaben, mit der Ausnahme für den Unterstützungszeitraum.

Nutzer müssen jedoch beachten, dass der Unterstützungszeitraum gemäß Konformitätserklärung und/oder den Betriebshandbüchern endet und es danach keine verpflichtenden Schwachstellenmeldungen und Security Updates für das PDE mehr gibt. Sollte das PDE nach dem Unterstützungszeitraum weiter betrieben werden, muss sich der Nutzer selbst um das Schwachstellenmanagement kümmern. Gerade im Businessbereich ist es daher ratsam, die Unterstützungszeiträume für verwendete PDEs im Auge zu behalten und sich schon beim Kauf eines PDEs eine Strategie für den Umgang mit dem Ende des Unterstützungszeitraumes zu überlegen. Folgende Strategien sind dabei üblich:

Austausch des PDEs vor Ende des Unterstützungszeitraums

Eine Möglichkeit ist es, PDEs vor dem Ende des Unterstützungszeitraumes auszuwechseln und somit immer im Unterstützungszeitraum der verwendeten PDEs zu bleiben. Bei dieser Strategie ist es essenziell, zu wissen, wann die Unterstützungszeiträume für die verwendeten PDEs enden und ausreichend Zeit einzuplanen, um Ersatz zu beschaffen.

Erweiterte Wartungsverträge abschließen

Bei manchen PDEs ist es möglich Wartungsverträge abzuschließen, die die Behandlung von Schwachstellen auch über das normale Ende der Unterstützungszeiträume hinweg garantieren. Dafür sollte jedoch der Zeitraum, in dem das PDE betrieben werden soll, möglichst genau bekannt sein, da die Wartungsverträge zumeist beim Kauf abgeschlossen werden müssen.

Weiterbetrieb ohne Unterstützung durch den Hersteller

Die dritte mögliche Strategie ist, ein PDE auch nach dem Ende der Unterstützung durch den Hersteller weiterzubetreiben. Hierbei ist jedoch zu beachten, dass der Hersteller nach dem Ende des Unterstützungszeitraumes auch nicht mehr für Schwachstellen im PDE haftbar gemacht werden kann. Zudem sollte der Betreiber sich erkundigen ob und wo er nach dem Unterstützungszeitraum Schwachstellen erhalten kann und wie er diese selbständig behandeln möchte.

3.3.6 Unterstützungsphase

Der Unterstützungszeitraum für das PDE beginnt spätestens mit der Fertigstellung des ersten Produkts der Serie. Ab diesem Zeitpunkt muss der Hersteller aktiv nach Schwachstellen seines PDEs suchen und selbst gefundene oder ihm gemeldete Sicherheitsprobleme (Schwachstellen) durch das Bereitstellen von Updates oder anderen geeigneten Maßnahmen beheben. Wurde das PDE noch nicht ausgeliefert kann der Hersteller die korrigierende Maßnahme (z. B. Security Patch) noch im Werk einspielen oder ein Security Update bereitlegen, das der Nutzer initial installiert (vgl. ➔ Kapitel 3.2.1 Auslieferung ohne bekannte Schwachstellen).

Der Hersteller ist verpflichtet, den Unterstützungszeitraum für jedes PDE so festzulegen, dass dieser der voraussichtlichen Nutzungsdauer entspricht ↗ CRA Artikel 13 (8). Für die Bestimmung sollten sie die folgenden Faktoren berücksichtigen:

- Angemessene Erwartungen der Nutzer;
- Die Art des PDEs, einschließlich seines Verwendungszwecks;
- Sonstige Unionsvorschriften, die die Lebensdauer von PDEs regeln.

Weitere relevante Faktoren, die Hersteller berücksichtigen können, sind:

- Den Unterstützungszeitraum ähnlicher PDEs, die von anderen Herstellern in Verkehr gebracht wurden;
- Die Verfügbarkeit der Betriebsumgebung;
- Den Unterstützungszeitraum integrierter Komponenten von Drittanbietern, die Kernfunktionen bereitstellen;
- Relevante Leitlinien der ADCO ↗ CRA Artikel 52 (15).

Alle aufgeführten Faktoren sollten so berücksichtigt werden, dass bei der Festlegung des Unterstützungszeitraums die Verhältnismäßigkeit gewährleistet ist. Beispielsweise können für die Festlegung des Unterstützungszeitraums bei Systemen nach ➔ Kapitel 2.3, die aus verschiedenen PDEs bestehen, die Unterstützungszeiträume der integrierten PDEs sowie ähnlicher PDEs berücksichtigt werden.

Die Mindestdauer für den Support beträgt fünf Jahre bzw. der erwarteten Nutzungsdauer des PDEs. Der Zeitraum kann je nach PDE auch über- oder unterschritten werden.

Die exakte Dauer des Unterstützungszeitraumes wird durch den Hersteller festgelegt und muss in leicht zugänglicher Weise mindestens mit Monat und Jahr kenntlich gemacht werden ↗ CRA Artikel 13 (11). Das angegebene Datum ist wie ein Mindesthaltbarkeitsdatum zu verstehen und kennzeichnet das früheste Ende der Unterstützung. Eine längere Unterstützung ist möglich, wenn das Produkt noch weiter produziert und vertrieben wird. Ebenso muss der Hersteller die

Informationen, welche er bei der Bestimmung des Unterstützungszeitraumes verwendet hat, in die technische Dokumentation gemäß ↗ CRA Anhang VII aufnehmen.

Sollten die durch die ADCO erhobenen Marktüberwachungsdaten auf unangemessene Unterstützungszeiträume hindeuten, so kann die EU-Kommission Rechtsakte erlassen, welche Mindestunterstützungszeiträume für bestimmte Produktkategorien festlegen.

Wichtig: Zudem ist zu beachten, dass die Unterstützungszeiträume für jedes PDE einzeln gelten. Dies bedeutet, dass die Unterstützung für eine Produktserie erst dann eingestellt werden kann, wenn der Unterstützungszeitraum für das letzte ausgelieferte Exemplar endet.

HINWEIS 1 Die Kommission wird weitere Leitlinien zu diesem Thema bereitstellen ↗ CRA Artikel 26.

HINWEIS 2 In B2B-Verträgen muss der Unterstützungszeitraum eindeutig angegeben sein.

HINWEIS 3 Der Unterstützungszeitraum kann auch einen geplanten Tausch von Hardware oder Software enthalten.

3.4 CRA und Zulassung

Im Kontext der Zulassung soll hier zunächst betrachtet werden, wann der CRA hinter anderen Rechtsvorschriften, unter anderem Zulassungsverfahren, zurücktritt:

1. Wenn andere EU-Rechtsakte Vorgaben enthalten, die den Regelungen aus dem CRA teilweise oder gänzlich entgegenstehen, ist eine Lösung des Konflikts herbeizuführen und dieser vollständig umzusetzen. Dies kann im Einzelfall bedeuten, dass Regelungen der jeweiligen Zulassungsverfahren den CRA in seiner Umsetzung einschränken. Das Vorgehen ist im Einzelfall zu prüfen.
2. Falls es sektorspezifische Vorschriften gibt, die das gleiche oder ein höheres Schutzniveau als der CRA bieten, so kann die EU-Kommission Rechtsakte erlassen, die diesen Sektor von der Anwendung des CRA befreien.

3.4.1 Zulassung/Rückwirkungsfreiheit

Zulassungsverfahren, andere Genehmigungsverfahren und die Konformität zum CRA sind getrennt zu betrachten. Die CRA-Konformität wird im Rahmen der CE-Kennzeichnung eigenverantwortlich sichergestellt. Ein erfolgreich durchgeführtes Zulassungsverfahren oder anderes Genehmigungsverfahren impliziert keine CRA-Konformität. Umgekehrt ist der Nachweis der CRA-Konformität (sowie die CE-Konformität) keine notwendige Voraussetzung für ein Zulassungs- oder anderes Genehmigungsverfahren, mit Ausnahme der Erklärung der CE-Konformität. Hierzu wird bspw. für Genehmigungsverfahren, die in den Anwendungsbereich der Interoperabilitätsrichtlinie (EU) 2016/707 fallen, nach Art. 13 Durchführungsverordnung (EU) 2018/545 der Prozess zur Erfassung der Anforderungen durchgeführt. Dieser stellt sicher, dass alle relevanten Vorschriften und Rechtsakte der EU betrachtet und entsprechend umgesetzt wurden.

Art. 2 Nr. 11 Durchführungsverordnung (EU) 2018/545:

> „Erfassung der Anforderungen“ den Prozess der Ermittlung, Zuweisung, Umsetzung und Validierung der Anforderungen, die der Antragsteller erfüllen muss, um sicherzustellen, dass die einschlägigen Vorschriften der Union und der Mitgliedstaaten eingehalten werden. Die Erfassung der Anforderungen kann im Rahmen der Produktentwicklungsprozesse erfolgen;“

Derzeit bestehen für das Zulassungsverfahren keine weitergehende gesetzliche Anforderung im Hinblick auf den CRA. Eine Pflicht zur Durchführung einer Bewertung durch Dritte (insbesondere durch eine notifizierte Stelle) besteht nur, wenn das PDE einer der gemäß CRA relevanten Produktklassen zugeordnet ist.

Sollten jedoch im Rahmen des Nachweises der CRA-Konformität Dokumentationen entstehen, die ebenfalls die Anforderungen von bestimmten Zulassungs- oder anderen Genehmigungsverfahren erfüllen oder umgekehrt, so können die einmal entstandenen Dokumentationen natürlich auch mehrfach verwendet werden.

Regelungen zu unabhängigen Prüfverfahren gemäß CRA sind in ➔ Kapitel 3.5.3 erläutert.

3.4.2 Updates im Kontext Zulassung/Anwendung CRA

In Hinsicht auf die Veränderung eines PDEs, stellt der CRA in den meisten Fällen eine Besonderheit gegenüber anderen Zulassungs- und Genehmigungsverfahren dar: Die meisten Verfahren prüfen ein neues PDE einmal vor der Einführung auf den Markt und diese Zulassung gilt dann, solange das PDE unverändert bleibt.

Der CRA hingegen fordert eine fortlaufende Veränderung des PDEs, wenngleich in einem stark beschränkten Rahmen, ohne dass eine erneute Bewertung notwendig wird. Diese im CRA geforderte Veränderung bezieht sich dabei auf Security Updates. Mit dem Begriff Security Updates sind hier Updates gemeint, die ausschließlich dazu dienen, die Cybersicherheit eines PDEs zu verbessern, die Funktionalität eines PDEs aber nicht berühren. In allen anderen Fällen gilt, dass analog zu den anderen Verfahren, eine erneute Prüfung und Bewertung der CRA-Konformität des PDEs notwendig wird.

Weiterhin stellt sich nun die Frage, ob Zulassungsverfahren und/oder andere Genehmigungsverfahren, durch die im CRA geforderten Security Updates beeinflusst werden. Da dies stark von dem jeweiligen PDE und den dazugehörigen Verfahren abhängt, kann in diesem Leitfaden keine allgemeine Aussage getroffen werden. Es ist von Fall zu Fall zu entscheiden.

Für weitere Details, die die Themen Software/Security-Update betreffen sei hier auf das ➔ Kapitel 3.2 verwiesen.

3.5 Ausstellung der Konformitätserklärung

3.5.1 Konformitätserklärung

Die Konformitätserklärung wird grundsätzlich durch den Hersteller eines PDEs mit digitalen Elementen selbst ausgestellt. Dies ist unter anderem darin begründet, dass es sich bei der Konformitätserklärung um eine schriftliche Zusicherung des Herstellers handelt, dass sein PDE konform ist.

Die Konformitätserklärung wird durch das ↗ CE-Zeichen ausgedrückt. Hierbei ist zu beachten, dass der CRA zunächst nur eine Konformitätserklärung fordert, die besagt, dass der CRA erfüllt wird. Sollte das PDE allerdings noch weiteren EU-Rechtsvorschriften unterliegen, die eine Konformitätserklärung vorschreiben, so ist insgesamt nur eine Konformitätserklärung zu erstellen ↗ CRA Artikel 28 (4), die die Konformität mit allen entsprechenden Rechtsvorschriften erklärt. Für den Inhalt der Konformitätserklärung bedeutet dies Folgendes:

Ist der CRA die einzige Rechtsvorschrift, die das PDE zu erfüllen hat, genügen die Vorgaben des CRAs für die Konformitätserklärung. Sollte das PDE weiteren Rechtsvorschriften unterliegen, die ebenfalls eine Konformitätserklärung erfordern, so sind die Vorgaben des CRAs für die Konformitätserklärung lediglich ergänzend zu den anderen Vorgaben für die Konformitätserklärung zu sehen.

Der CRA selbst fordert dabei in ↗ CRA Anhang V die folgenden acht Inhalte:

1. Mindestens den Namen und Typen eines PDEs. Sollten diese nicht ausreichen, um das PDE eindeutig zu identifizieren, müssen weitere Informationen hinzugefügt werden, die eine eindeutige Identifizierung ermöglichen. Im Falle einer Serienproduktion wäre es zum Beispiel die Seriennummer des PDEs.
2. Den Namen und die Anschrift des Herstellers oder gegebenenfalls seines Bevollmächtigten.
3. Eine Erklärung des Anbieters, die besagt, dass dieser die alleinige Verantwortung für die Ausstellung der EU-Konformitätserklärung trägt.
4. Den Gegenstand der Erklärung, hier die Produktbezeichnung. Gegebenenfalls ist auch ein Foto einzufügen.
5. Eine Erklärung, dass das PDE den einschlägigen Harmonisierungsvorschriften der EU entspricht.
6. Eine Auflistung aller Normen, Vorschriften und Zertifizierungen, zu denen die Konformität erklärt wird.
7. Eine Beschreibung des durchgeführten Konformitätsbewertungsverfahrens und die Kennnummer der ausgestellten Bescheinigung. Sollte das Verfahren durch eine notifizierte Stelle durchgeführt werden, dann muss auch die Kennnummer der notifizierten Stelle angegeben werden.
8. „Unterzeichnet für und im Namen von:
   - (Ort und Datum der Ausstellung)
   - (Name, Funktion) (Unterschrift):“

Ist die oben beschriebene Konformitätserklärung zu umfangreich, um sie dem PDE beizulegen, kann eine vereinfachte Konformitätserklärung erstellt und beigelegt werden. Diese ersetzt die vollständige Konformitätserklärung jedoch nicht, sondern stellt lediglich einen formellen Verweis auf die vollständige Erklärung dar. Für die vereinfachte Konformitätserklärung ist der nachfolgende Textbaustein aus CRA Anhang VI zu verwenden:

BEISPIEL

Beispiel zur vereinfachten Konformitätserklärung:

„Hiermit erklärt ... [Name des Herstellers], dass der Typ des Produkts mit digitalen Elementen ... [Bezeichnung des Typs des PDEs mit digitalen Elementen] der Verordnung (EU) 2024/2847 entspricht.

Der vollständige Text der EU-Konformitätserklärung kann unter der folgenden Internetadresse abgerufen werden: ...“

Unabhängig von der Konformitätserklärung ist die Technische Dokumentation nach CRA Artikel 31 und Anhang VII verpflichtend bereit zu stellen. In dieser Dokumentation sind die Anwendungsbedingungen, unter welchen die CRA-Konformität gilt und erhalten bleibt, zu dokumentieren.

3.5.2 Technische Dokumentation

Für jedes PDE mit digitalen Elementen ist neben der Konformitätserklärung ebenso eine technische Dokumentation zu erstellen. Analog zur Konformitätserklärung gibt es für jedes PDE genau eine technische Dokumentation, in der nicht nur die durch den CRA vorgeschriebenen Inhalte enthalten sein sollen, sondern auch etwaige Inhalte, die durch andere EU-Rechtsvorschriften gefordert werden.

Bevor nun auf die Inhalte der technischen Dokumentation eingegangen wird, sei noch darauf hingewiesen, dass eine unvollständige oder fehlende technische Dokumentation gemäß CRA Artikel 58 (1f) eine formale Nicht-Konformität darstellen kann. Dies kann eine Einschränkung oder sogar ein Verbot für die weitere Bereitstellung auf dem Markt inklusive Rückruf zur Folge haben.

Die Inhalte, die der CRA von der technischen Dokumentation zum Zeitpunkt der Erstellung dieses Leitfadens fordert, sind im CRA Anhang VII des CRAs definiert und sollen im nachfolgenden zusammengefasst wiedergegeben werden. Gemäß CRA Artikel 31 (5) ist die Kommission jedoch berechtigt weitere verpflichtende Elemente in die technische Dokumentation aufzunehmen, weshalb wir empfehlen, CRA Anhang VII selbstständig und regelmäßig auf Aktualisierungen zu prüfen.

Zusammenfassung der vorgeschriebenen Inhalte der technischen Dokumentation:

- Eine allgemeine Beschreibung des PDEs mit digitalen Elementen, inklusive der Zweckbestimmung, Softwareversionen, soweit möglich Fotos und Abbildungen der Hardware und die in CRA Anhang II beschriebenen Anleitungen und Informationen für die Nutzer des PDEs.

- Beschreibung der Konzeption, Entwicklung und Herstellung des PDEs aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen, zusammenwirken und sich in der Gesamtverarbeitung integrieren.
- Beschreibung der erforderlichen Informationen und Spezifikationen die das Schwachstellenmanagement umfassen, einschließlich SBOM, Konzept zur Offenlegung, Nachweis einer Kontaktadresse zur Meldung von Schwachstellen und technische Beschreibung eines sicheren Verbreitungsweges für Security Updates.
- Informationen und Spezifikationen bezüglich Herstellungs- und Überwachsprozessen und deren Validierung.
- Bewertung der im gesamten Lebenszyklus berücksichtigten Cybersicherheitsrisiken, inklusive der Frage inwieweit die Cybersicherheitsanforderungen aus ↗ CRA Anhang I Anwendung finden.
- Einschlägige Informationen, die bei der Festlegung des Unterstützungszeitraumes berücksichtigt wurden.
- Beschreibung der Lösungen mit denen die Anforderungen aus ↗ CRA Anhang I und II erfüllt werden. Unter Beachtung und Angabe von harmonisierten Normen und Spezifikationen.
- Berichte über Tests und Prüfungen, mit denen die Erfüllung der Anforderungen an das PDE und das Schwachstellenmanagement geprüft wurden.
- Ein Exemplar der Konformitätserklärung.
- Auf Verlangen der Marktüberwachungsbehörde ein Exemplar der SBOM.

Ist die technische Dokumentation erstellt muss sie, je nachdem, was länger ist, für 10 Jahre nach dem Inverkehrbringen des PDEs oder die Dauer des Unterstützungszeitraums aufbewahrt werden. Zuständig für die Aufbewahrung der technischen Dokumentation können der Hersteller, sein Bevollmächtigter oder ein Einführer sein, hier ist entscheidend, wer das PDE auf dem europäischen Markt in Verkehr bringt.

3.5.3 Konformitätsbewertungsverfahren

	Default	Wichtig I	Wichtig II	Kritisch
Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle	✖			
Selbsteinschätzung, wenn harmonisierter Standard angewendet werden kann		✖		
EU-Baumusterprüfung + Konformität mit dem Baumuster auf der Grundlage einer internen Fertigungskontrolle (inkludiert Prüfung durch notifizierte Stelle)		✖	✖	✖
Konformität auf der Grundlage einer umfassenden Qualitätssicherung (inkludiert Prüfung durch notifizierte Stelle)		✖	✖	✖

Tabelle 15: Konformitätsbewertungsverfahren

Die CRA-Konformität eines PDEs wird grundsätzlich durch die Konformitätserklärung zugesichert. Dennoch schreibt der CRA für die Sicherstellung der Konformität die Verwendung eines europäischen Schemas für Cybersicherheitszertifizierung einer der dem PDE entsprechenden Klasse vor. Sollte ein solches Schema jedoch nicht verfügbar sein, so muss, je

nach Produktklasse, mindestens eines der im ↗ CRA Anhang VIII beschriebenen vier Konformitätsbewertungsverfahren verwendet werden.

Die Zuordnung der Konformitätsbewertungsverfahren kann aus der nachfolgenden ➔ Tabelle 15 entnommen werden. Entsprechend ➔ Kapitel 2.5 sind Bahnprodukte in der Regel in der Klasse „default“ angesiedelt.

4 Fallbeispiele

4.1 Inverkehrbringen und Bereitstellung von Produkten nach dem 11.12.2027

4.1.1 Verantwortlichkeiten, Kaskade-Schwachstellen und Updates

Im ersten Beispiel soll anhand einer HVAC, die in einem Zug verbaut wird, verdeutlicht werden, wie der CRA den Umgang mit Schwachstellenmeldungen und den dazugehörigen Updates regelt, wenn alle PDEs nach dem 11.12.2027 hergestellt wurden und somit dem CRA unterliegen. Zudem werden noch einige Hinweise gegeben, die den Umgang mit dieser Regelung vereinfachen sollen. In einem zweiten Beispiel wird das Szenario dahingehend verändert, dass ein Teil der PDEs schon vor dem 11.12.2027 hergestellt wurden und somit nicht dem CRA unterliegen.

FALLBEISPIEL 1

Wie aus ➔ Abbildung 14 ersichtlich wird, handelt es sich sowohl bei dem Hersteller von Teilsystemen als auch bei dem Integrator aus Sicht der CRAs um Hersteller von Produkten mit digitalen Elementen. Dies bedeutet, beide sind verpflichtet Sicherheitsprobleme (z. B. Schwachstellen) in ihren jeweiligen PDEs zu identifizieren, diese zu bewerten, die erforderlichen Maßnahmen zu deren Behebung zu ergreifen und die Nutzer zu informieren, sobald ein Security-Update zur Verfügung steht. Dem Integrator kommt hierbei eine Sonderrolle zu, da er aus Sicht des CRAs zwar Hersteller des Zuges ist, aber gleichzeitig auch Nutzer der HVAC. Dies bedeutet auch, dass zwischen dem Hersteller des HVACs und Nutzer im Sinne des CRA keine Geschäftsbeziehung besteht, außer es wird explizit anders vertraglich vereinbart. Dem Betreiber, im Sinne des CRA der Nutzer (➔ Kapitel 2.2.1), gegenüber ist nur der Integrator verantwortlich. Die Verpflichtung Informationen weiterzugeben, besteht nur dem jeweils eigenen Nutzer gegenüber. In diesem Beispiel bedeutet dies, dass der Hersteller des HVACs den Integrator über Schwachstellen der HVAC und der Integrator den Nutzer über Schwachstellen des Zuges informiert.

Die in der ➔ Abbildung 14 dargestellte Bestätigung der Informationen und Akzeptanz der jeweiligen Lösungen ist durch den CRA nicht vorgeschrieben, wird durch diesen Leitfaden aber empfohlen. Der Hintergrund ist, dass der CRA auf Konsumprodukte ausgelegt ist, bei denen der Hersteller die Nutzer nicht zwangsläufig kennt. In weiten Bereichen der Bahnindustrie ist dies anders, wodurch es möglich ist, auf konkrete Umstände der Integration einzugehen. Diese Bestätigung kann zum einen helfen, Haftungsfragen im Vorfeld eindeutig zu klären und zum anderen bietet sie dem jeweiligen Nutzer die Möglichkeit, auf eine bessere Lösung zu bestehen. Das Vorgehen ist also in beidseitigem Interesse.

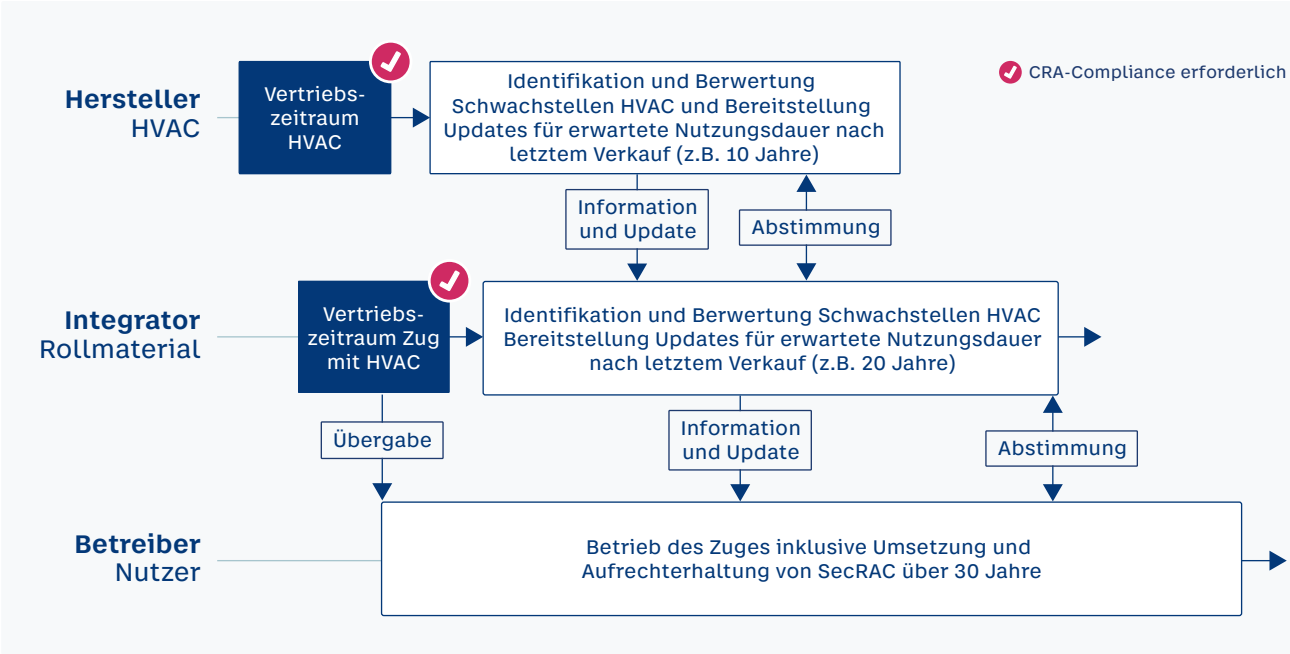

Abbildung 14: Verantwortlichkeiten Fallbeispiel 1

Eine weitere Verpflichtung, die der CRA den Herstellern auferlegt, ist die Identifikation von Schwachstellen und deren Behebung über einen bestimmten Zeitraum sicherzustellen. Der vorgeschriebene Zeitraum entspricht dabei der vernünftigerweise zu erwartenden Nutzungsdauer des jeweiligen PDEs. Das Wort PDE bezieht sich dabei auf jedes einzelne hergestellte PDE und nicht auf die Produktserie. Der vereinbarte Unterstützungszeitraum, innerhalb dessen Maßnahmen zur Behebung sicherheitsrelevanter Probleme bereitzustellen sind, beginnt erst nach Auslieferung der letzten HVAC zu laufen. Das heißt, der Zeitpunkt der Auslieferung des letzten Produktes einer Baureihe markiert den Start einer vollen Unterstützungsperiode. Hierbei ist zu beachten, dass die zu erwartende Nutzungsdauer nicht immer der tatsächlichen Nutzungsdauer des jeweiligen Betreibers entsprechen muss. Wie in der ➔ Abbildung 14 dargestellt kann es sein, dass die HVAC eine Nutzungsdauer von 10 Jahren vorsieht, der Zug eine Nutzungsdauer von 20 Jahren und der Nutzer den Zug tatsächlich 30 Jahre nutzen möchte. Wie in der ➔ Abbildung 14 ersichtlich entsteht durch die unterschiedlichen Zeiträume in denen Schwachstellenmeldungen und Lösungen bereitgestellt werden nun ein Problem für den Integrator. Dieser erhält ab einem bestimmten Zeitpunkt keine Schwachstellenmeldungen und Lösungen für die HVAC mehr, muss diese aber selbst weiterhin an den Nutzer liefern. Es ist also ratsam, sich bereits bei der Entwicklung eines Produktes Gedanken zu machen, bei welchen zugekauften Komponenten dieses Problem auftreten könnte und wie man es lösen möchte. Hierzu stünden beispielsweise folgende Lösungsoptionen zur Verfügung:

- Es könnte mit dem Hersteller vertraglich die Dauer des Unterstützungszeitraumes und die Art der Maßnahmen, z. B. Schwachstellenidentifikation und eine festgelegte Anzahl von SW-Updates, vereinbart werden.
- Es könnte mit dem Hersteller der HVAC vertraglich vereinbart werden, dass dieser spätestens nach Ende der Unterstützungsphase die SBOM der HVAC und ggf. weitere Informationen, die zur Identifikation und Behandlung von Schwachstellen notwendig sind, an den Integrator übergibt, damit er sich selbstständig um einen Abgleich mit einer Schwachstellendatenbank kümmern und die Behebung der Schwachstellen bei Bedarf ermöglichen kann. In der vertraglichen Regelung kann auch eine Regelung zur Ver-

schwiegenheit über die Geschäftsgeheimnisse des HVAC-Herstellers enthalten sein. Es muss sichergestellt werden, dass die Rechte am geistigen Eigentum gewahrt bleiben.

- Es könnte mit dem Nutzer im Wartungskonzept die Wahl risikobasierter Maßnahmen nach Abschluss des vorgesehenen Unterstützungszeitraums, z. B. einen Ersatz des betroffenen Produkts, vereinbart werden.

FALLBEISPIEL 2

Das zweite Beispiel unterscheidet sich vom Ersten in dem Punkt, dass die HVAC bereits vor Inkrafttreten des CRA erworben wurde und somit nicht dem CRA unterliegt. Auch die Entwicklung des Zugs selbst liegt bereits in der Vergangenheit. Die HVAC muss demnach keine Security-Anforderungen gemäß CRA umsetzen. Der integrierte Zug muss diese jedoch erfüllen, auch wenn die Entwicklung des HVACs bereits Jahre zurückliegt. Der Integrator hat damit die Verantwortung auf Systemebene (Zug), die CRA-Konformität sicherzustellen. Die Unterstützung durch Hersteller sollte bilateral geregelt werden.

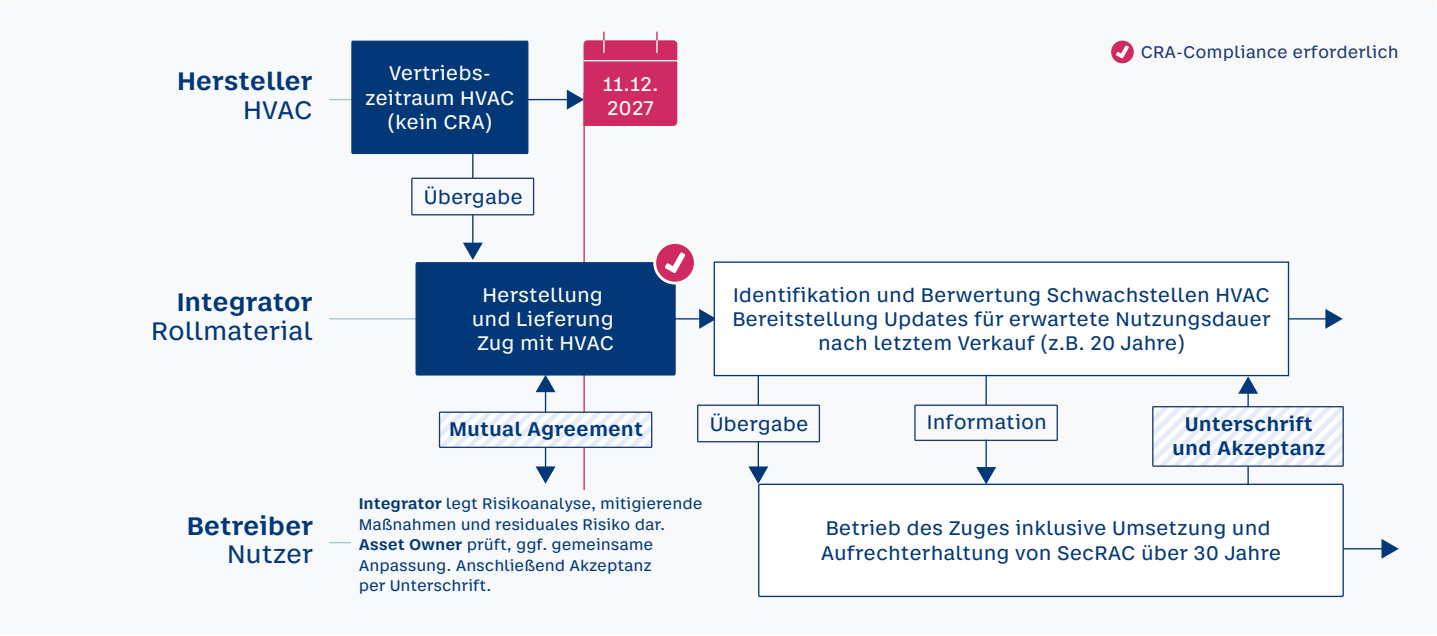

Abbildung 15: Verantwortlichkeiten Fallbeispiel 2

Für das Management der CRA-Compliance auf Systemebene wird die Risikoanalyse, durchgeführt durch den Integrator, mit Nennung von mitigierenden Maßnahmen und des verbleibenden Restrisikos. Die Informationen zum Restrisiko und Maßnahmen, die teilweise auch Anwendungsbedingungen auf Seite des Nutzers sein können, legt der Integrator dem Nutzer vor. Der Nutzer wird dann gebeten, die Risikoanalyse zu prüfen und gegebenenfalls mit dem Integrator zusammen weitere Maßnahmen zu beschließen. In einer gemeinsamen Vereinbarung werden die vereinbarten Maßnahmen und Restrisiken festgehalten. Das gerade beschriebene Verfahren wird in diesem Leitfaden als Mutual Agreement (➔ Kapitel 2.12) bezeichnet und ist als Übergangslösung für den Zeitraum gedacht, in dem noch Produkte verbaut werden könnten, die bereits vor dem Inkrafttreten des CRA erworben wurden.

Der Integrator stellt die Konformitätserklärung gemeinsam mit der technischen Dokumentation aus, die alle Anwendungsbedingungen und Restrisiken ausweist. Das Mutual Agreement erlaubt keinen Verantwortungsübergang. Das Mutual Agreement ist nur für Projekte gedacht, die vor Inkrafttreten des CRA unterzeichnet wurden. (vgl. ➔ Kapitel 2.12)

4.1.2 Produkte aus mehreren Komponenten

Bei vielen Produkten handelt es sich um Komponenten, Teilsysteme oder Systeme, die aus diversen Bestandteilen zusammengesetzt werden. Dabei werden nicht alle Bestandteile eines solchen PDEs durch den Hersteller, der das gesamte Produkt verkauft, hergestellt. Oft wird auch ein Teil der eingesetzten Komponenten von Dritten zugekauft und verwendet. Hierdurch stellt sich die Frage, in welchem Fall ein Zulieferer und in welchem Fall der Hersteller des gesamten Konstruktes die Pflichten, die der CRA dem Hersteller auferlegt, erfüllen muss. Dies soll anhand des Beispiels einer HVAC-Steuerung in den nachfolgenden Beispielen erläutert werden.

FALLBEISPIEL 1

HVAC-Steuerung wird mit vorinstallierter Applikationssoftware (App) oder Applikationssoftware (App) im Bundle verkauft.

In diesem Beispiel wird eine HVAC-Steuerung mit einer vorinstallierten App oder einer App im Bundle (geliefert z. B. als Download) verkauft. Die Steuerung ist dabei nicht separat erhältlich und wird von einem Dritten (Komponenten-Hersteller) zugekauft:

In diesem Fall muss die CRA-Konformität der Steuerung zwar durch den Komponenten-Hersteller bereits einmal sichergestellt und erklärt werden, der Integrator muss aber dennoch die CRA-Konformität für das komplette System, bestehend aus Steuerung und App, erneut prüfen, sicherstellen und erklären. Es genügt nicht, dies nur für die App zu tun. Er kann und soll sich aber auf die in der Dokumentation enthaltenen Informationen der Steuerung des Komponenten-Herstellers stützen.

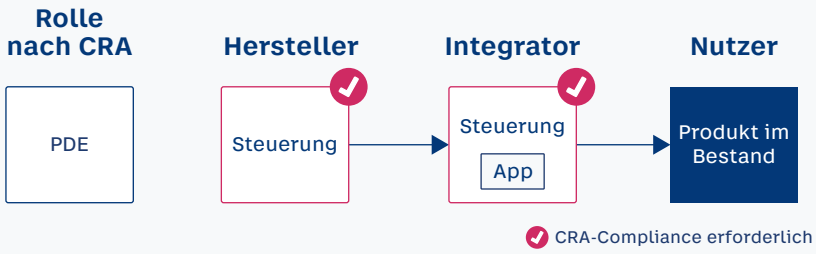

Abbildung 16: Produkte aus mehreren Komponenten Fallbeispiel 1

FALLBEISPIEL 2

Steuerung und App werden separat angeboten und verkauft.

In diesem Beispiel werden die HVAC-Steuerung und die App separat verkauft. Die App kann zwar auf der Steuerung installiert werden, ist aber nicht zwingend für die Funktion erforderlich. Weiterhin gilt, dass die Steuerung durch den App-Anbieter von einem Dritten (Komponenten-Hersteller) zugekauft und unverändert weiterverkauft wird:

Hier ist der Komponenten-Hersteller für die CRA-Konformität der Steuerung zuständig und der Hersteller der App für die CRA-Konformität der App. Der App-Anbieter agiert aber als Händler und hat damit die Pflicht zu prüfen, ob die CRA-Konformität vorliegt (↗ CRA Artikel 20). Er muss diese aber inhaltlich nicht prüfen oder neu erklären, sofern er keine Änderungen vornimmt und damit zum Integrator wird.

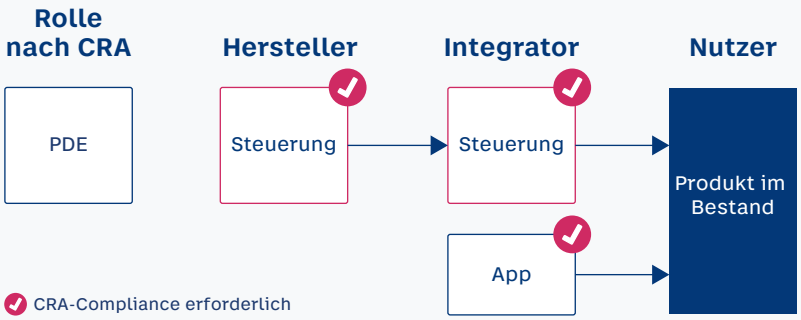

Abbildung 17: Produkte aus mehreren Komponenten Fallbeispiel 2

FALLBEISPIEL 3

HVAC-System wird inklusive aller Komponenten zur Integration in einen Zug angeboten

In diesem Beispiel wird nicht nur die HVAC-Steuerung, sondern das ganze System zusammen verkauft, damit es in dieser Konfiguration in einem Zug verbaut werden kann. Im Anschluss daran wird der Zug ebenfalls verkauft:

Zunächst gilt hier wieder, dass der Komponenten-Hersteller der Steuerung wieder für die CRA-Konformität der Steuerung zuständig ist.

Da das HVAC-System als Ganzes angeboten wird, muss der Hersteller des HVAC-Systems hier die CRA-Konformität für das gesamte System, inklusive Steuerung, App, allen Aktoren und Sensoren sicherstellen und mit Ausstellung einer Konformitätserklärung bescheinigen. Es ist dabei nicht notwendig die CRA-Konformität für die einzelnen Komponenten zu erklären, insofern sie nicht separat vertrieben werden. Die Sicherstellung vom CRA und Cybersicherheit entlang der Lieferkette ist aber im Interesse des Herstellers. Die Prüfung, Sicherstellung und Erklärung der CRA-Konformität für das gesamte System ist ausreichend. Dabei ist wieder der vorgesehene und vernünftigerweise vorhersehbare Nutzen für die Bewertung entscheidend. Schutzmaßnahmen in einem Zug (mechanischer Schutz, physischer Schutz, ...) können angenommen und in der Dokumentation für den Anwender bzw. Integrator des Zuges dokumentiert werden.

Der Hersteller des Zuges (Integrator des HVACs) muss wiederrum die CRA-Konformität des Zuges als Ganzes sicherstellen, da der Zug wieder als neues PDE gilt.

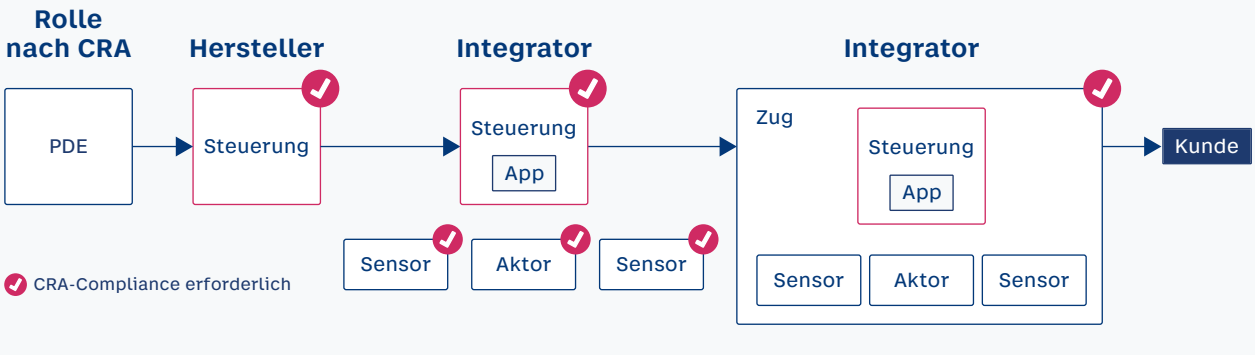

Abbildung 18: Produkte aus mehreren Komponenten Fallbeispiel 3

FALLBEISPIEL 4

Komponenten eines HVAC-Systems werden nach dem Baukastensystem angeboten

In diesem Beispiel werden die Komponenten eines HVAC-Systems separat angeboten. Dies kann zum Beispiel in einem Webshop erfolgen, in dem der Hersteller eines Zuges die Steuerung, die Aktoren und Sensoren, die er benötigt einzeln erwerben kann. Im Falle der HVAC-Steuerung gilt, dass sie von einem Dritten zugekauft wird, aber nur zusammen mit einer App erworben werden kann (für die Steuerung inklusive App gilt Fallbeispiel 1):

Für den Hersteller des HVAC-Systems gilt nun, dass dieser für jede Komponente einzeln die CRA-Konformität herstellen und erklären muss, da jede Komponente einzeln erworben werden kann. Der vorgesehene und vernünftigerweise vorhersehbare Nutzen kann hier deutlich weiter gefasst sein, als im Fallbeispiel 3. Abhilfe kann eine deutliche Einschränkung des erklärten Anwendungsbereichs der einzeln angebotenen Sensoren und Aktoren sein, um wieder Gebrauch von Schutzmaßnahmen (vgl. Fallbeispiel 3) machen zu können.

Der Hersteller des Zuges muss im Anschluss wiederrum die CRA-Konformität des Zuges herstellen und erklären, da der Zug als neues PDE gilt.

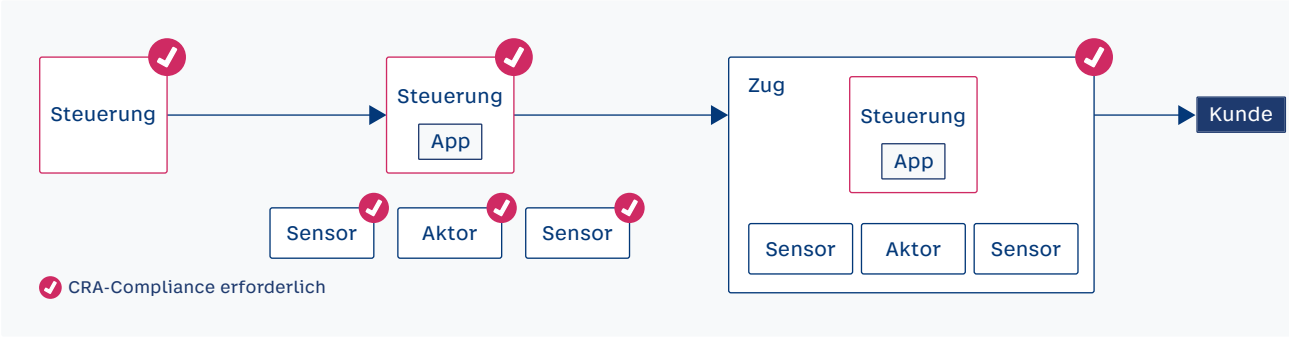

Abbildung 19: Produkte aus mehreren Komponenten Fallbeispiel 4

4.1.3 Bestandsprodukte

Bestandsprodukte werden oft auf zwei Arten interpretiert.

1. Existierende Produkte

Existierende Produkte, z. B. ein Schienenfahrzeug, fallen nicht unter den CRA, solange sie vor dem 11.12.2027 in Verkehr gebracht wurden (➔ Kapitel 2.4) und seitdem keine substanzielle Veränderung (➔ Kapitel 2.9) erfahren haben. Diese Produkte können auch zwischendurch weiterveräußert werden, ohne CRA-Anforderungen erfüllen zu müssen.

FALLBEISPIEL 1

Ein Systemintegrator bringt im Oktober 2006 ein Schienenfahrzeug (Rollmaterial) in Verkehr. Der Betreiber A betreibt dieses Rollmaterial bis November 2028. Im Dezember 2028 veräußert der Betreiber das Rollmaterial ohne technische Erneuerung (abgesehen von Ersatzteilen) an einen anderen Betreiber B innerhalb der EU. Das Rollmaterial wird durch den Betreiber – hier in der Rolle des Händlers – erneut auf dem Markt bereitgestellt. Das Rollmaterial muss den CRA nicht erfüllen, da es bereits vor dem 11.12.2027 in Verkehr gebracht wurde und keine substanziellen Veränderungen daran vorgenommen wurden.

FALLBEISPIEL 2

Der neue Betreiber B aus Fallbeispiel 1 integriert ein neues Fahrgastinformationssystem in das Rollmaterial. Das Fahrgastinformationssystem muss den CRA erfüllen. Der Betreiber fungiert als Integrator (oder beauftragt einen Integrator). Dieser muss auch die Prüfung nach ➔ Kapitel 2.9 durchführen, ob weitere Anteile des Rollmaterials durch die substanzielle Veränderung betroffen sind.

2. Entwickelte und eingeführte Produktserien

Ein Integrator hat ein Rollmaterial entwickelt und 2022 das erste Stück der geplanten Serie erstmalig in Verkehr gebracht. 2026 bestellt ein Betreiber dieses Produkt nach. Die Herstellung und Inverkehrbringen erfolgt im März 2028. Das technisch identische Produkt muss im Jahr 2028 den CRA erfüllen.

Es ist unerheblich, wann ein Produkt entwickelt, genehmigt oder bestellt wurde. Es ist ausschließlich relevant, zu welchem Zeitpunkt das Produkt in Verkehr gebracht wird (➔ Kapitel 2.4).

Handelt es sich wiederum um eine Lieferung, welche bereits im Vertrag von 2022 vereinbart wurde, so kann die CRA-Erfüllung durch Anwendung des projektbasierten Ansatzes (➔ Kapitel 2.11) in Verbindung mit dem Mutual Agreement (➔ Kapitel 2.12) für eine Auslieferung im Jahr 2028 erfolgen.

Soll ein identischer Abruf, welcher als **Option im Vertrag** von 2022 vereinbart wurde, im Jahr 2028 erfolgen, so muss der CRA erfüllt werden. Der **projektbasierten Ansatz** (➔ Kapitel 2.11) und das **Mutual Agreement** (➔ Kapitel 2.12) sind hier **nicht anwendbar**, weil die konkrete Lieferung nicht fest vereinbart war.

Jedes einzelne Produkt wird in Verkehr gebracht. Produktserien sind nicht relevant für diese Bewertung (➔ Kapitel 2.4).

4.1.4 Austauschkomponenten/Ersatzbeschaffung

Werden Ersatzteile beschafft, bedürfen diese keiner CRA-Compliance. Weiterhin ergeben sich keine Auswirkungen auf die CRA-Compliance des Zuges. Allerdings kann eine Ersatzbeschaffung plötzlich selbst CRA-relevant sein, wenn sie neue Funktionen integriert. Um als Ersatzteile zu gelten, müssen die Anforderungen aus ➔ Kapitel 2.10 eingehalten werden. Folgend sind verschiedene Fallbeispiele, die auch Grenzfälle darstellen, aufgeführt.

FALLBEISPIEL 1

Ein Zug, der im Jahr 2005 in Verkehr gebracht wurde, erhält 2028 einen Ersatz des Bremsensystems, da es sein Lebensende erreicht hat. Das Bremsensystem wird noch funktionsgleich hergestellt und ist als Ersatzteil verfügbar. CRA muss nicht angewendet werden.

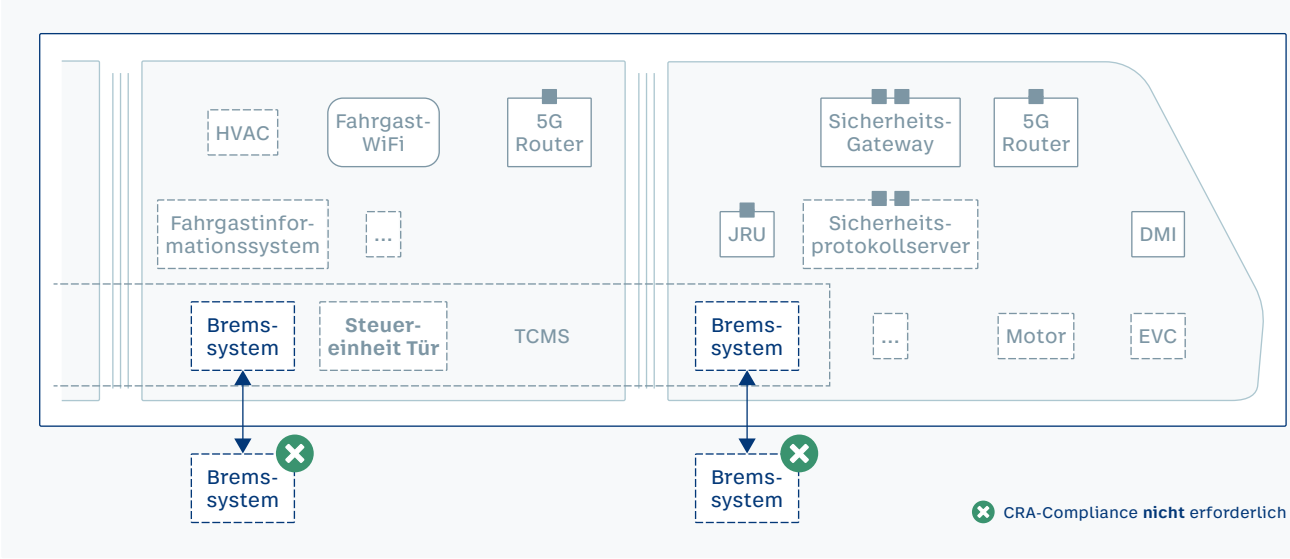

Abbildung 20: Ersatzteil funktionsgleich

FALLBEISPIEL 2

Ein Zug, der im Jahr 2005 in Verkehr gebracht wurde, erhält 2028 einen Ersatz des Bremsensystems, da es sein Lebensende erreicht hat. Das Ersatzteil ist nicht mehr vorhanden. Auch ein funktionsgleiches Ersatzteil ist nicht vorhanden. Allerdings ist ein kompatibles, neues Bremssystem vorhanden. Dieses ist nun bereits CRA konform. Der Einbau kann erfolgen.

Es erfolgt durch den Integrator (Eigentümer, Betreiber, beauftragter Integrator) die Prüfung, ob die neue Komponente rechtliche Auswirkungen auf das Fahrzeug hinsichtlich substanzieller Veränderungen hat. Dies ist nicht der Fall, denn es werden die alten Schnittstellen verwendet und keine neuen Kommunikationskanäle in den Zug integriert.

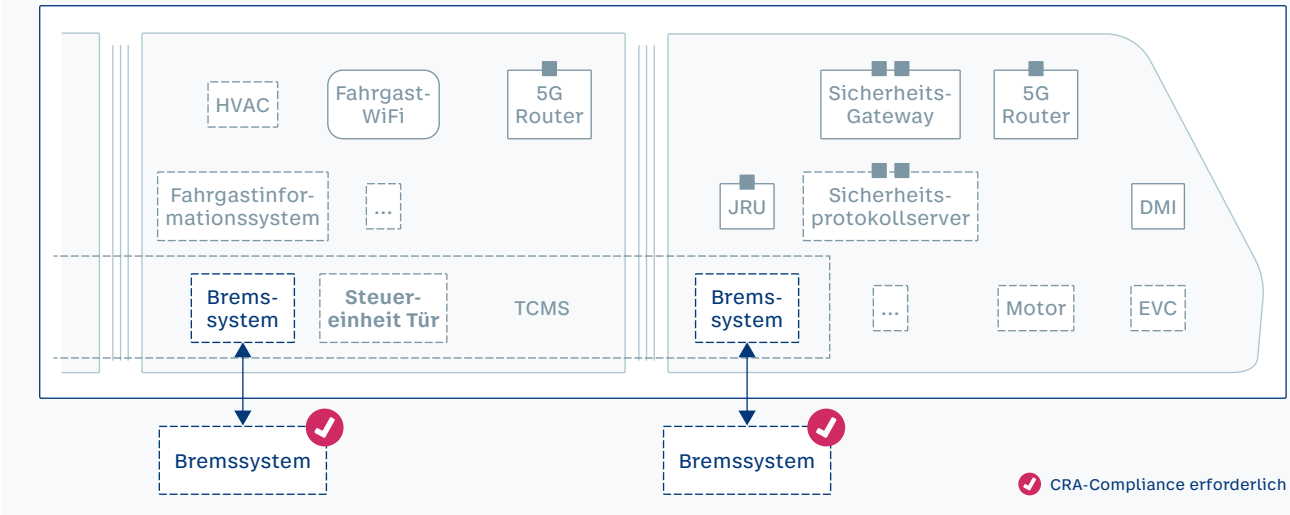

Abbildung 21: Ersatzteil neu, CRA konform

FALLBEISPIEL 3

Ein Zug, der im Jahr 2005 in Verkehr gebracht wurde, erhält 2028 einen Ersatz des Bremsensystems, da es sein Lebensende erreicht hat. Das Ersatzteil ist nicht mehr vorhanden. Auch ein funktionsgleiches Ersatzteil ist nicht vorhanden. Allerdings ist ein kompatibles, neues Bremssystem vorhanden. Dieses ist nun bereits CRA-konform. Der Einbau kann erfolgen. Es erfolgt durch den Integrator (Eigentümer, Betreiber, beauftragter Integrator) die Prüfung, ob

die neue Komponente rechtliche Auswirkungen auf das Fahrzeug hinsichtlich substanzieller Veränderungen hat.

Das neue Bremssystem bringt neue Schnittstellen zum TCMS mit, um optimierte Fahr- und Bremsoptionen durch ein Software-Update für das zukünftig geplante ATO verwenden zu können. Die Erneuerung mit scheinbar einem Ersatzteil hat nun Auswirkungen auf das Fahrzeug. Diese müssen bewertet und Maßnahmen entsprechend ➔ Kapitel 2.9 ergriffen werden.

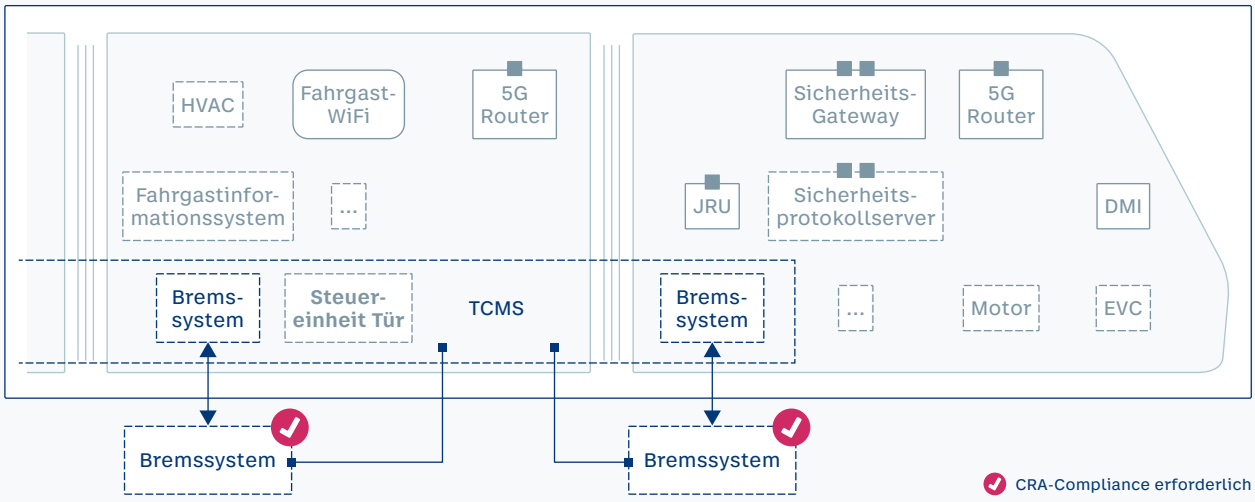

Abbildung 22: Ersatzteil neu, CRA-konform, neue Schnittstellen in das Fahrzeug

4.1.5 Reparatur von Anlagen/Systemen

Die Reparatur von Anlagen ist im CRA nicht geregelt. Jedoch wird darauf in den Erwägungsgründen 29, 39 und 42 eingegangen.

- In Erwägungsgrund 29 wird die Reparatur in den Kontext zum Ersatzteil gesetzt. Diese Anwendung entspricht damit ➔ Kapitel 2.10 sowie den Beispielen aus ➔ Kapitel 4.1.4.
- In Erwägungsgrund 42 wird die Reparatur mit „Wartung“ und „Überholung“ genannt.
- In Erwägungsgrund 39 wird die Reparatur auch auf Software angewendet.

In allen Fällen können Reparaturen vergleichend Ersatzteilen behandelt werden, solange sie die Kernfunktion nicht verändern und die Cybersicherheit nicht negativ beeinflussen.

In der praktischen Erwägung ist:

- eine physische Reparatur als mechanische Handlung an einem digitalen Produkt zu betrachten, dass nicht vollständig ersetzt wird.
- eine Reparatur einer Software als Patch zu betrachten, der eine Fehlfunktion (bug) behebt.

4.1.6 Kompatible Systemerweiterung (Retrofit)

Nachfolgend wird als Beispiel für das ➔ Kapitel 2.14 ein neuer Umbauvertrag als kompatible Systemerweiterung (Retrofit) behandelt. Die Herstellung findet nach dem 11.12.2027 statt.

Im Projekt wird ein sich im Einsatz befindlicher Triebzug um einen weiteren Mittelwagen mit darin befindlichen PDEs ergänzt (➔ Abbildung 23). Die geplanten zu integrierenden Mittelwagen sind in diesem Aufbau bereits in einer anderen Flotte in Betrieb. Es handelt sich daher um ein Beispiel für in ➔ Kapitel 2.14 genannt: „Neuer Wagen in einem Zugverband, der mit dem Rest des bestehenden Zugverbands interagieren muss“.

Abbildung 23: Retrofit: Neuer Mittelwagen wird in Triebzug eingefügt

Technische Herausforderung:

- Funktionale Kompatibilität der Teilsysteme zwischen dem bestehenden Triebzug und dem weiteren Mittelwagen (Leittechnik, Bremse, Türsystem, Video, etc.).
- Auswirkung potenziell unterschiedlicher Stände Richtung Cybersicherheit von funktional gleichen Teilsysteme zwischen dem bestehenden Triebzug und dem weiteren Mittelwagen.

Durch den Einbau von gleichen oder schnittstellenkompatiblen Teilsystemen wird die Kompatibilität zwischen dem bestehenden Triebzug und dem weiteren Mittelwagen nach dem Umbau aufrechterhalten. Für mögliche Abweichungen zum CRA sind die Schritte nach ➔ Kapitel 2.8 umzusetzen. Die ➔ Abbildung 24 stellt drei Fallbeispiele für die Integration von PDEs in den neuen Mittelwagen dar.

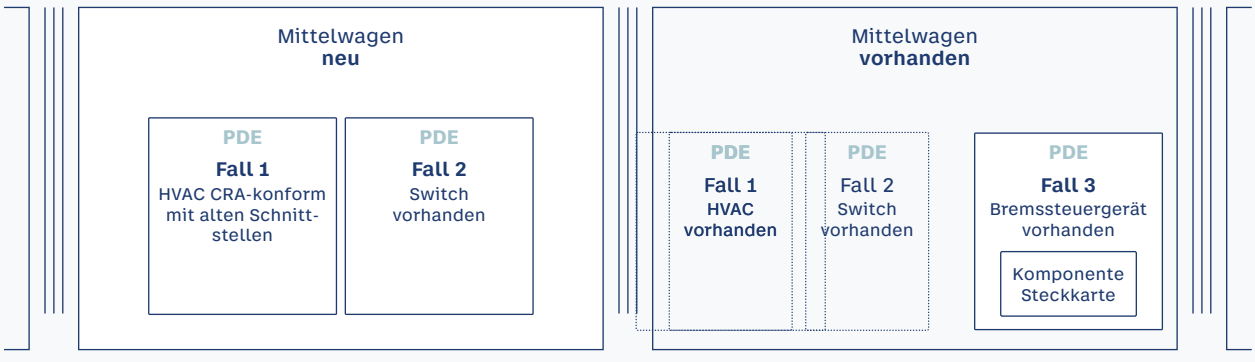

Abbildung 24: Drei Beispiele für die Integration von PDEs in neuen Mittelwagen

FALL 1

Ein HVAC wird in den neuen Mittelwagen integriert, welches vom Hersteller mit funktionaler Kompatibilität zum vorhandenen Triebzug geliefert werden kann und den CRA als Teilsystem erfüllt. Die neue HVAC erfüllt den CRA ohne Einschränkungen, abgesehen von der Nutzung einer alten Kommunikationsschnittstelle mit der zentralen Steuerung. Für die Kompatibilität wird die Konfiguration des neuen HVAC entsprechend angepasst, damit die gleichen Schnittstellen zum Triebzug realisiert werden können.

FALL 2

Ein CRA-konformer Switch kann nicht mit den vorhandenen Switchen kommunizieren. Deshalb wird der alte Switch gewählt und eingebaut. Es wird eine Risikoanalyse durchgeführt, geprüft, ob und wenn ja, welche mitigierenden Maßnahmen getroffen werden können oder müssen. Dies wird begründet in der technischen Dokumentation niedergeschrieben und entsprechend umgesetzt.

FALL 3

Das Teilsystem (Bremssteuergerät) im vorhandenen Wagen wird um eine Komponente (Steckkarte zur Signalverarbeitung) erweitert. Damit wird allein die Kapazität ausgeweitet, aber keine neue Funktionalität hinzugefügt und auch die Security nicht negativ beeinflusst (vgl. ➔ Kapitel 2.9). Dies wird begründet in der technischen Dokumentation niedergeschrieben.

5 Hilfestellungen und deren Einordnung für den Bahnsektor

5.1 BSI (TR-03183)

Folgend sind kurz die wesentlichen Informationen zum BSI TR-03183 zusammengestellt. Der Text stammt von der Website des BSI[17].

> „Die BSI TR-03183 ist als Sammlung von Informationen und als Einstiegshilfe in den CRA gedacht. Zielgruppe sind insbesondere Hersteller, die noch keine ausgereiften IT-Sicherheitsprozesse im Rahmen ihrer Entwicklung und Schwachstellenbehandlung etabliert haben.
>
> Dieses Dokument stellt eine Hilfestellung ohne verpflichtenden oder verbindlichen Charakter dar. Es kann nicht für eine Konformitätsvermutung genutzt werden. Die BSI TR-03183 wird sukzessive weiterentwickelt und durch die korrespondierenden harmonisierten Europäischen Standards ersetzt, sobald diese bereitstehen.
>
> Der CRA ist im Dezember 2024 in Kraft getreten. Aktuell laufen die Übergangsfristen bis zur vollständigen Umsetzung am 11. Dezember 2027.
>
> Die Technische Richtlinie wird kontinuierlich aktualisiert und weiterentwickelt.“

In ↗ Teil 1 „General Requirements“ werden Anforderungen an Hersteller und Produkte in Anlehnung an die Anforderungen aus Artikeln und Anhängen des CRA zusammengestellt.

In ↗ Teil 2 „Software Bill of Materials (SBOM)“ werden formelle und fachliche Vorgaben für SBOM beschrieben.

In ↗ Teil 3 „Vulnerability Reports and Notifications“ wird der Umgang mit eingehenden Schwachstellenmeldungen beschrieben.

17 www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html

5.2 ERJU System Pillar

Die ERJU System Pillar ist ein europäisches Projekt mit dem Ziel, eine einheitliche europäische Eisenbahnlandschaft zu schaffen (Single European Railway Area – SERA). Das Projekt fokussiert sich dabei auf die bahnbetrieblich relevanten und zumeist sicherheitsrelevanten oder sicherheitsnahen Systeme. Darin enthalten sind alle Systeme des sogenannten ZSS (Zugsicherungssystems), das heißt:

- Stellwerke
- Außenelemente
- Bediensysteme
- Traffic Management Systeme
- ETCS
- Zugsicherungssysteme auf dem Fahrzeug (EVC, DMI, TCMS, ...)
- Gleisarbeiter-Sicherheitssysteme

Darüber hinaus werden transversale Themen und operationelle Themen behandelt. Das sind unter anderem:

- Einheitliche Betriebsordnung
- Software-Update-Prozesse
- Security
- Zulassung und Performance Prozesse (PRAMS)

Alle Arbeitsgruppen (Domains) arbeiten in einem paritätischen Prinzip bestehend aus Experten für die jeweiligen Domänen der Hersteller und Betreiber.

In dieser Initiative existiert die Security Domain. Das Ziel der Security Domain ist die zentrale Bereitstellung von Security Anforderungen für alle Systeme in dem genannten Scope. Für dieses Ziel wurde ein generisches Konzept der „Secure Component“ entwickelt. Eine Secure Component kann eine Hardware oder Software sein und ist durch die eigene Anwendung, ihre Schnittstellen und Umgebungsbedingungen, wie Einhausung etc. gekennzeichnet. Beispielsweise sind Stellwerke, Feldelementcontroller, Bahnübergänge, RBC, usw. jeweils eine Secure Component.

Es wird grundsätzlich angenommen, dass alle Netzverbindungen offene Netze sind. Das heißt, es kann von keinem Security-Schutz der Netze für die Anwendung ausgegangen werden. Es wird konsequent Ende-zu-Ende-Security angewendet.

Basierend auf einer Risikoanalyse und einer Zonierung für die Architektur wurden die Spezifikationen basierend auf der IEC 62443-3-3 bzw. -4-2 entwickelt. Diese lauten:

- Shared Cybersecurity Services Specification
- Secure Communication Specification
- Secure Component Specification
- Security Program Requirements

Neben den vier Spezifikationen wurden weitere unterstützende Dokumente entwickelt und veröffentlicht. Den letzten Stand aller Unterlagen kann man jederzeit hier in der Sektion „Security“ einsehen ↗ https://rail-research.europa.eu/horizontal-tasks

Neben der Entwicklung basierend auf IEC 62443 stellen die Spezifikationen ein Tracing für die folgenden Standards bereit:

- CRA – Cyber Resilience Act
- CSA – Cyber Security Act
- NIS 2
- IEC 63452 (aktueller Entwurf)/TS 50701

Die Anwendung der System Pillar Cybersecurity Spezifikation kann daher direkt herangezogen werden, um die technischen Anforderungen nach CRA erfolgreich umzusetzen. Die Anwendbarkeit ist nicht auf den oben genannten Scope begrenzt. Durch die Generik als „Protection Profile“ kann sie auf quasi jede Komponente angewendet werden. Die folgende ➔ Abbildung 25 zeigt den Zusammenhang auf.

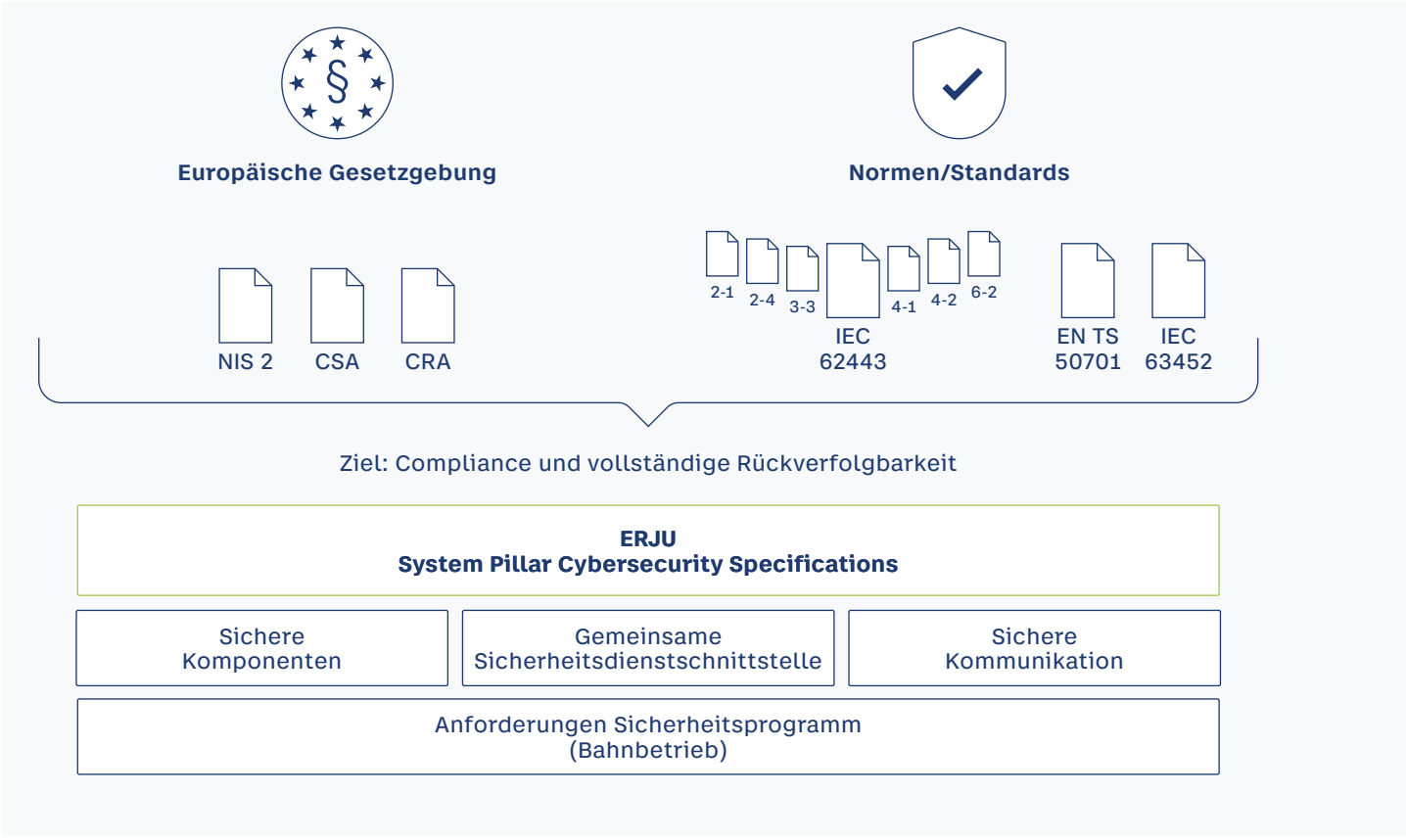

Abbildung 25: System Pillar Cybersecurity

Tabellenverzeichnis

Abbildungsverzeichnis

Impressum

Herausgeber
© 05/2026
Verband der Bahnindustrie in Deutschland (VDB) e.V.
Universitätsstraße 2, 10117 Berlin
Lobbyregister Nr. R003287

+49 30 206289-0
info@bahnindustrie.info
bahnindustrie.info
The German Railway Industry Association VDB
Bahnindustrie_D

Bildnachweise
Titelbild: ©freepik.com

Entwurf und Gestaltung
webersupiran.berlin

Der Verband der Bahnindustrie in Deutschland (VDB) e. V.

vertritt die Interessen von über 250 Unternehmen, von weltweit führenden Systemhäusern ebenso wie von spezialisierten mittelständischen „Hidden Champions". Die Mitglieder des VDB entwickeln und fertigen Systeme und Komponenten für Schienenfahrzeuge und Infrastruktur mit rund 56.600 Mitarbeiterinnen und Mitarbeitern allein in Deutschland. Innovative Technologien „Made in Germany" sorgen weltweit für exzellente Bahnsysteme, klimaschonende Mobilität und digitale Innovationen.

Die Bahnindustrie.

Verband der Bahnindustrie in Deutschland

bahnindustrie.info