Was bedeutet der Cyber Resilience Act (CRA) für den Bahnsektor?

What does the Cyber Resilience Act (CRA) mean for the railway sector?

Martin Koop

Die Sicherheit des Bahnbetriebs ist eine gemeinsame Leistung. Sie erfordert einerseits sichere Betriebsprozesse, eine sichere Betriebsumgebung sowie eine kontinuierliche Erhaltung dieses Zustands. Andererseits müssen die Produkte dieses Maß an Sicherheit unterstützen. In der Safety ist dies seit über 100 Jahren Standard. In der Security wurden bisher vor allem die Betreiber (KRITIS, NIS) in die Pflicht genommen. Der Cyber Resilience Act (CRA) fordert nun von allen Produktherstellern nachzuziehen und ein Mindestmaß einzuhalten. Wie klappt der schnelle Paradigmenwechsel bis Ende 2027?

1 Einleitung: Cybersicherheit als systemrelevante Aufgabe

Die Bahn ist eine der zentralen Kritischen Infrastrukturen Europas. Sie verbindet Volkswirtschaften, ermöglicht den Transport von Millionen von Menschen und Milliarden Tonnen Gütern und gilt im Rahmen der NIS2-Richtlinie wie auch nationaler Sicherheitsgesetze als besonders schutzwürdig. Während Sicherheit im Bahnbereich traditionell mit der Safety von Zügen, Infrastruktur und Betriebssystemen verbunden war, hat sich das Bild in den letzten Jahren grundlegend gewandelt: Cybersecurity ist zu einem zentralen Anforderungsbestandteil der Bahnsicherheit geworden.
Der steigende Einsatz von digitalen Steuerungs- und Kommunikationssystemen (ETCS, FRMCS, TCMS, ATO usw.) vergrößert die Angriffsfläche erheblich. Ransomware-Angriffe auf Verkehrsunternehmen, die Störung von Signaltechnik oder gezielte Attacken auf Fahrgast- und Ticketingsysteme zeigen, wie real die Bedrohung ist. Der CRA setzt hier an: Mit ihm hat die Europäische Union eine horizontal gültige Regulierung geschaffen, die vor allem die Hersteller, aber auch Betreiber digitaler Produkte stärker in die Pflicht nimmt.
Für den Bahnsektor stellt der CRA eine Zäsur dar: Einerseits eröffnet er die Chance, ein harmonisiertes Mindestniveau an Cybersicherheit durchzusetzen. Andererseits kollidieren die Regelungen mit den langen Lebenszyklen, komplexen Lieferketten und hohen Sicherheitsanforderungen der Branche.
Der Beitrag soll einen Überblick über die wesentlichen Aspekte des CRA und seine Anwendung im Bahnsektor geben sowie einen Ausblick auf nächste Schritte.

2 Der CRA im Überblick

Der Cyber Resilience Act (Regulation EU 2024/2847) trat am 10. Dezember 2024 in Kraft und wird ab 11. Dezember 2027 vollumfänglich anwendbar. Sein Kernziel: digitale Produkte sicherer

Railway safety is a joint effort. On the one hand, it requires safe operating processes, a safe operating environment and continuous maintenance of this state. On the other hand, products must support this level of safety. This has been standard safety practice for over 100 years. In the case of security, it has primarily been the operators (KRITIS, NIS) who have been held accountable. The Cyber Resilience Act (CRA) now requires all product manufacturers to follow suit and comply with the minimum standards. How will this rapid paradigm shift work by the end of 2027?

1 Introduction: cybersecurity as a system-relevant task

Railways are one of Europe's key critical infrastructures. They connect economies, enable the transport of millions of people and billions of tonnes of goods and are considered particularly worthy of protection under the NIS2 Directive and national security laws. While safety in the railway sector has traditionally been associated with the safety of trains, infrastructure and operating systems, the picture has changed fundamentally in recent years: cybersecurity has now become a central component of railway safety requirements.
The increasing use of digital control and communication systems (ETCS, FRMCS, TCMS, ATO, etc.) has significantly increased the attack surface. Ransomware attacks on transport companies, the disruption of signalling technology and targeted attacks on passenger and ticketing systems show how real the threat is. This is where the CRA comes in: with it, the European Union has created a horizontally applicable regulation that places greater responsibility on manufacturers in particular, but also on the operators of digital products.
The CRA represents a turning point for the rail sector: on the one hand, it opens up an opportunity to enforce a harmonised minimum level of cybersecurity. On the other hand, the regulations clash with the long lifecycles, complex supply chains and high security requirements in the industry.
This article aims to provide an overview of the key aspects of the CRA and its application in the railway sector, as well as an outlook regarding the next steps.

2 The CRA at a glance

The Cyber Resilience Act (Regulation EU 2024/2847) came into force on 10 December 2024 and will be fully applicable from 11 December 2027. Its core objective is to make digital products

machen, indem Produkte bereits unter Security-Gesichtspunkten entwickelt werden, damit Sicherheitslücken systematisch verhindert und über den Lebenszyklus entdeckt und geschlossen werden.
Zur Umsetzung dieser Ziele verfolgt der CRA einige Grundprinzipien. Auf diese wird später genauer im Bezug zum Bahnsektor eingegangen.

2.1 Produkt mit digitalen Elementen

Dies ist „ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden" (Art 3.1, CRA).

2.2 Grundprinzipien des CRA

- Security by Design & by Default: Produkte mit digitalen Elementen (PDE) müssen von Beginn an mit geeigneten Security-Maßnahmen entwickelt werden.
- Risikomanagement: Hersteller müssen potenzielle Cybersecurity-Risiken identifizieren, die bei der vorgesehenen Verwendung auftreten können, dokumentieren und über den gesamten Lebenszyklus nachhalten.
- Patch- und Updatepflichten: Hersteller müssen für den vorgesehenen Unterstützungszeitraum, jedoch mindestens für fünf Jahre, Sicherheitsupdates kostenfrei bereitstellen.
- Meldepflichten: Sicherheitsvorfälle und aktiv ausgenutzte Schwachstellen sind innerhalb von 24 Stunden an ENISA (European Union Agency for Cybersecurity) und das nationale CSIRT (Cyber Security Incident Response Team) zu melden.
- Verantwortlichkeiten entlang der Lieferkette: Neben Herstellern sind auch Importeure und Distributoren adressiert. Wer ein Produkt wesentlich verändert oder unter eigenem Namen vertreibt, gilt als Hersteller mit allen Pflichten des CRA.

2.3 Zeitpunkte

- 11. September 2026: Reporting-Pflichten treten in Kraft. Ab diesem Datum müssen alle aktiv ausgenutzten Schwachstellen aller Produkte gemeldet werden. Das umfasst auch bereits auf dem Markt befindliche Produkte.
- 11. Dezember 2027: Ab diesem Datum muss jedes auf dem EU-Markt bereitgestellte Produkt eine CRA-Konformitätserklärung haben. Dieser wird durch ein CE-Zeichen Ausdruck verliehen. Das CE-Zeichen muss nicht auf dem Gerät angebracht sein, sondern kann auch auf der Verpackung angebracht oder nur als Zusatzinformation im Liefervertrag angegeben sein. Die Konformitätserklärung muss einsehbar sein. Das kann z. B. durch Bereitstellung auf der Website des Herstellers erfolgen.
- 11. Juni 2028: Gibt es bereits security-zertifizierte Produkte basierend auf anderen harmonisierten Standards, verlieren diese im Sinne des CRA hier ihre Gültigkeit. Ab jetzt ist (zusätzlich) die CRA-Konformität erforderlich. Hinweis: Die IEC 62443 ist kein solch harmonisierter Standard.

2.4 Produktklassen

Der CRA unterscheidet vier Klassen (Default, Important I, Important II, Critical):

- Standard (Default): Eine Selbsterklärung genügt.
- Wichtige Klasse I (Important I): Selbsterklärung möglich, wenn ein harmonisierter Standard vorhanden ist. Gilt zwingend für Systeme wie IAM (Identity and Access Management), PKI (Public Key Infrastructure), SIEM (Security Information and Event Management System), 5G und FRMCS.

more secure by developing products with security in mind, so that any security gaps are systematically prevented, detected and closed throughout a product's lifecycle.
The CRA pursues a number of basic principles to achieve these objectives. These will be discussed in more detail later in relation to the railway sector.

2.1 Products with digital elements

This involves "a software or hardware product and its remote data processing solutions, including software or hardware components that are placed on the market separately" (Art. 3.1, CRA).

2.2 The basic principles of the CRA

- Security by Design & by Default: products with digital elements (PDE) must be developed with appropriate security measures from the very beginning.
- Risk management: manufacturers must identify, document and track any potential cybersecurity risks that may arise during the intended use throughout the entire lifecycle.
- Patch and update obligations: manufacturers must provide security updates free of charge for the intended support period, but at least for five years.
- Reporting obligations: any security incidents and actively exploited vulnerabilities must be reported to ENISA (European Union Agency for Cybersecurity) and the national CSIRT (Cyber Security Incident Response Team) within 24 hours.
- Responsibilities along the supply chain: in addition to manufacturers, importers and distributors are also addressed. Anyone who significantly modifies a product or distributes it under their own name is considered to be a manufacturer with all the obligations of the CRA.

2.3 Timing

- 11 September 2026: the reporting obligations will come into force. From this date onwards, all actively exploited vulnerabilities in all products must be reported. This also includes products already on the market.
- 11 December 2027: from this date onwards, every product made available on the EU market must have a CRA declaration of conformity. This is expressed by a CE mark. The CE mark does not have to be affixed to the device, but can also be affixed to the packaging or simply provided as additional information in the delivery contract. The declaration of conformity must be accessible. This can be achieved, for example, by making it available on the manufacturer's website.
- 11 June 2028: any security-certified products based on other harmonised standards will lose their validity under the CRA. From now on, CRA conformity will be (additionally) required. Note: IEC 62443 does not count as such a harmonised standard.

2.4 Product classes

The CRA distinguishes between four classes (Default, Important I, Important II, Critical):

- Default: a self-declaration is sufficient.
- Important Class I: self-declaration is possible if a harmonised standard is available. Mandatory for systems such as IAM (Identity and Access Management), PKI (Public Key Infrastructure), SIEM (Security Information and Event Management System), 5G and FRMCS.

- Wichtige Klasse II (Important II): Zwingend externe Konformitätsbewertung. Gilt zwingend für Firewalls, IDS, IPS, Hypervisors, Container und Tamper resistente Prozessoren.
- Kritisch (Critical:) Zwingend externe Konformitätsbewertung. Gilt zwingend für HSM (Hardware Security Module), TPM (Trusted Platform Module), Smart Meter Gateways und Smartcards.

3 Umsetzung im Bahnsektor

3.1 Besonderheiten des Bahnsektors

Die Umsetzung des CRA im Bahnsektor ist kein einfaches Übertragen von IT-Regeln, sondern erfordert eine differenzierte und strategische Betrachtung. Einfache Gründe dafür sind kurz aufgeführt:

- Lebenszyklen von 25 – 50 Jahren: Signaltechnik oder Rollmaterial laufen über Jahrzehnte stabil, während Cyberbedrohungen sich alle Monate ändern.
- Projektlaufzeiten von bis zu 20 Jahren: Lieferverträge, die vor dem Inkrafttreten des CRA geschlossen wurden, laufen in vielen Fällen deutlich über 2028 hinaus. Ein prominentes Beispiel ist die Lieferung der neuen ICE. Im Mai 2023 vereinbart und mit einer vorgesehen Lieferung von 2026 bis 2030.
- Hohe Interoperabilitätsanforderungen: Durch TSI, ERTMS / ETCS und nationale Systeme müssen Züge und Infrastruktur generationenübergreifend kompatibel sein. Gewisse Anforderungen lassen sich dadurch nicht umsetzen, ohne die notwendige Interoperabilität zu verletzen.
- Sicherheitskritische Systeme: Safety-Systeme erfordern Cybersecurity, um ihre Eigenschaften in Summe dauerhaft aufrecht zu erhalten. Doch ihr heutiges Design kann oft noch als monolithisch bezeichnet werden. Änderungen im Lebenszyklus, z. B. für Updates, bedürfen Änderungen, die wiederum einen langwierigen Zulassungsprozess nach sich ziehen.

Diese Rahmenbedingungen führen dazu, dass der CRA ohne eine sektorspezifische Übersetzung zu Blockaden und Rechtsunsicherheit führen könnte. Diese Herausforderung wurde international und national erkannt und hat zu zwei, permanent im Austausch stehenden, Initiativen geführt:

- Die Cybersecurity Rail Sector Group (CSRG) wurde 2024 ins Leben gerufen und wird durch Experten der CER, EIM, UNIFE, UITP und EUG betrieben. Das erste Fokus-Thema dieser Gruppe ist der CRA. Eine erste Version einer Leitlinie wird im November 2025 erwartet.
- Der Arbeitskreis Cyber- und Informationssicherheit (CIS) des VDB ist im Januar 2025 gestartet. Die Arbeitsgruppe entstammt dem AK Mittelstand und hat ebenfalls den CRA als dringlichstes Thema identifiziert. Der erste Entwurf der Guideline wird hier Ende 2025 erwartet.

Die Guidelines werden umfangreich die Interpretationen des CRA für den Bahnsektor darstellen und teils anhand von Beispielen die konkrete Anwendung skizzieren. In diesem Beitrag wird auf einige wesentliche Punkte eingegangen, die sich direkt aus dem CRA ergeben und bereits eine wesentliche Hilfestellung darstellen können.

3.2 Anwendung des CRA im Bahnbereich

3.2.1 Produkte mit digitalen Elementen (PDE)

Nach CRA sind PDE jede Hardware- oder Softwarekomponente, die als Einheit auf den Markt kommt. Im Bahnumfeld zählen dazu:

- Komponenten, wie Türsteuerungen, Bordcomputer, Kameras, Ticketautomaten

- Important Class II: an external conformity assessment is mandatory. Mandatory for firewalls, IDS, IPS, hypervisors, containers and tamper-resistant processors.
- Critical: a mandatory external conformity assessment. Mandatory for HSM (Hardware Security Module), TPM (Trusted Platform Module), smart meter gateways and smart cards.

3 Implementation in the railway sector

3.1 Special features of the railway sector

Implementing the CRA in the railway sector is not simply a matter of transferring IT rules, but requires a differentiated and strategic approach. The simple reasons for this are briefly listed below:

- Lifecycles of 25 – 50 years: signalling technology and rolling stock remain stable for decades, while cyber threats change every few months.
- Project durations of up to 20 years: supply contracts concluded before the CRA came into force will in many cases run well beyond 2028. A prominent example is the delivery of the new ICE trains. Agreed in May 2023 with delivery scheduled for 2026 to 2030.
- High interoperability requirements: TSIs, ERTMS / ETCS and national systems require trains and infrastructure to be compatible across generations. Certain requirements cannot be implemented without compromising the necessary interoperability.
- Safety-critical systems: safety systems require cybersecurity in order to maintain their overall properties over the long term. However, their current design can often still be described as monolithic. Changes during the lifecycle, e.g. for updates, require modifications, which in turn entail a lengthy approval process.

These framework conditions mean that without sector-specific translation, the CRA could lead to blockages and legal uncertainty. This challenge has been recognised internationally and nationally and has led to the establishment of two initiatives that are now in constant dialogue:

- The Cybersecurity Rail Sector Group (CSRG) was launched in 2024 and is run by experts from CER, EIM, UNIFE, UITP and EUG. The first focus topic of this group is the CRA. The first version of a guideline is expected in November 2025.
- The VDB's Cyber and Information Security (CIS) working group was launched in January 2025. The working group originated from the SME working group and has also identified CRA as its most pressing issue. The first draft of the guideline is expected here at the end of 2025.

The guidelines will provide a comprehensive overview as to how to interpret the CRA for the railway sector and will outline specific applications, in some cases using examples. This article discusses a number of key points that arise directly from the CRA and can already provide significant assistance.

3.2 Applying the CRA in the railway sector

3.2.1 Products with digital elements (PDE)

According to the CRA, PDE are any hardware or software components that are marketed as a unit. In the railway environment, these include:

- components such as door controls, on-board computers, cameras, ticket machines

- Subsysteme, wie ETCS-OBU, SCADA-Systeme, Brandmeldeanlagen
- Systeme, wie Fahrzeuge (Rolling stock), Stellwerke, Unterwerke.

Nicht als PDE gelten Infrastrukturteile wie Tunnel oder Bahnhöfe – sie bestehen aus bzw. beinhalten PDE, sind aber selbst kein Produkt im Sinne des CRA. Weiterhin sind frei konfigurierbare Kombinationen in Summe kein Produkt nach CRA, sondern bestehen nur aus solchen. Das gilt z. B. für IC-Züge, deren Wagen und Lokomotiven je CRA relevant sind, aber in Kombination frei zusammenstellbar sind.
Wird eine Komponente durch einen System-Integrator eingekauft, so hat dieser zunächst darauf zu achten, dass diese als CRA-konform gekennzeichnet ist. Im zweiten Schritt hat er für die Integration ins System die Konformitätserklärung zu berücksichtigen, da darin die Anwendungsbestimmungen festgehalten sind, unter welchen das Produkt CRA-konform ist. Für das final integrierte Produkt hat der Integrator dann wiederum die CRA-Konformität zu bestätigen. Er kann sich dafür auf die Erklärungen der integrierten Komponenten stützen. Alle Nebenbestimmungen müssen behandelt sein oder sich in der Konformitätserklärung des Systems wiederfinden.

3.2.2 Produktklassen im Bahnkontext

Alle Eisenbahnprodukte können als Standardklasse betrachtet werden, es sei denn, sie werden ausdrücklich in einer der höheren Klassen, z. B. eine PKI oder ein TPM, erwähnt. Dies liegt daran, dass sich „Kritikalität" in diesem Zusammenhang nur auf die Cyberkritikalität bezieht. Sie steht in keinem Zusammenhang mit KRITIS.
Darüber hinaus ist es wichtig zu verstehen, dass es keine Vererbung in irgendeiner Richtung gibt. Eine Türsteuerungseinheit, in die ein TPM integriert ist, führt also nicht zu der Schlussfolgerung, dass die Türsteuerungseinheit zur kritischen Klasse gehört. Das TPM muss, wenn es in der EU verfügbar ist, die für die kritische Klasse festgelegten Bewertungskriterien erfüllen. Die Türsteuerung bleibt in der Standardklasse.

3.2.3 Zeitpunkte

Der 11. September 2026 ist noch weniger als ein Jahr hin und hat bereits eine Anforderung mit großer Auswirkung, aber – vermutlich – zunächst geringer Häufigkeit, verglichen mit existierenden Schwachstellen. Es müssen alle aktiv ausgenutzten Schwachstellen durch bösartige Angreifer an die zentrale Meldestelle (CSIRT national, ENISA) gemeldet werden. Und dies ist für alle digitalen Produkte, auch solche die bereits seit 20 Jahren oder mehr auf dem Markt sind, gültig. Jedoch muss dafür kein Monitoring eingerichtet werden, denn es geht um Kenntniserlangung. D. h., folgende Aktionen sind erforderlich:

- Einrichtung einer Kommunikationsstelle, z. B. Mailadresse oder Telefonnummer auf der Website, unter welcher dem eigenen Unternehmen solche Vorfälle gemeldet werden können.
- Einrichtung eines Prozesses, dass diese Informationen kurzfristig geprüft werden und bei Validität innerhalb von 24 Stunden eine Information an die zentrale Meldestelle ergehen kann.

Erst ab dem 11. Dezember 2027 ist ein Schwachstellen-Monitoring und die Bereitstellung von Lösungen (Patches) erforderlich. Und dieses gilt dann ausschließlich für Produkte, die ab 11. Dezember 2027 auf dem Markt bereitgestellt wurden. Beide Meldeanforderungen laufen ab dann parallel weiter.

3.3 Inverkehrbringung und Bereitstellung auf dem Markt

Die Inverkehrbringung ist die erstmalige Bereitstellung auf dem Markt der Europäischen Union. Ein Produkt kann durch einen Distributor weitere Male bereitgestellt werden.

- subsystems such as ETCS OBU, SCADA systems, fire alarm systems
- systems such as rolling stock, signal boxes, substations.

Infrastructure components such as tunnels or stations are not considered to be PDE: they consist of or contain PDE, but are not themselves products within the meaning of the CRA. Furthermore, freely configurable combinations are themselves not products according to the CRA, but merely consist of such products. This applies, for example, to IC trains, whose carriages and locomotives are relevant according to the CRA, but can be freely combined.
If a component is purchased via a system integrator, said integrator must first ensure that it is marked as being CRA-compliant. In a second step, they must take the declaration of conformity into account for integration into the system, as this contains the application provisions under which the product is CRA-compliant. The integrator must then confirm CRA compliance for the final integrated product. They can rely on the declarations of the integrated components to do this. All ancillary provisions must be addressed or included in the system's declaration of conformity.

3.2.2 Product classes within the rail context

All railway products may be considered as the default class, except for those cases where they are explicitly mentioned in one of the higher classes, e.g. a PKI or a TPM. This is because "criticality" within this context only refers to cyber criticality. It bears no relation to KRITIS.
In addition, it is important to understand that inheritance does not exist in any direction. So, a door control unit integrating a TPM does not lead to the conclusion that the door control unit falls within the critical class. If it is available in the EU, the TPM has to comply with the evaluation criteria set out for the critical class. The door controller stays in the default class.

3.2.3 Dates

11 September 2026 is less than a year away and already has a requirement with a major impact, but a, presumably, low frequency for the time being compared to the existence of the vulnerabilities. All the vulnerabilities actively exploited by malicious attackers must be reported to the central reporting office (CSIRT national, ENISA). And this applies to all digital products, even those that have been on the market for 20 years or more. However, no monitoring needs to be established for this, as it is a matter of gaining knowledge. This means that the following actions are required:

- The establishment of a communication point, e.g. an email address or telephone number on the website, where such incidents can be reported to your own company.
- The establishment of a process to ensure that this information is regularly checked and, if valid, can be forwarded to the central reporting centre within 24 hours.

Vulnerability monitoring and the provision of solutions (patches) will only be required from 11 December 2027 onwards. And this will then apply exclusively to products that have been launched onto the market from 11 December 2027 onwards. Both reporting requirements will continue to run in parallel from then on.

3.3 Market placement and market launches

Market placement refers to the initial provision in the European Union market. A product may be further provided by a distributor.

Die Bereitstellung auf dem Markt ist gekennzeichnet durch:
- Das physische Vorhandensein, d. h. das Produkt ist hergestellt und hat eine eindeutige Identifikationsnummer.
- Ein Angebot auf dem Markt, d. h. in Form eines Katalogs oder eines konkreten Angebots an einen Kunden (b2b).

Jedes einzelne Werkstück ist ein Produkt. D. h., jede einzeln hergestellte Entität desselben Typs wird in Verkehr gebracht. Dass dies nach der immer selben Spezifikation, einer bestehenden Zulassung oder Genehmigung passiert, ist im Sinne des CRA nicht relevant. So ist es zutreffend, dass ein, der technischen Gestaltung nach, identisches Produkt am 10. Dezember 2027 nicht-CRA-konform in Verkehr gebracht werden kann, am 11. Dezember 2027 jedoch die CRA-Konformität erforderlich ist.

3.4 Ersatzteile

Ersatzteile sind grundsätzlich vom CRA ausgenommen, sofern sie identisch oder funktional gleichwertig sind. Neu entwickelte Ersatzteile mit zusätzlichen Funktionen benötigen dagegen CRA-Konformität.

Es empfiehlt sich trotzdem, frühzeitig über CRA-konforme Ersatzteile nachzudenken. Denn ändert sich über den Lebenszyklus eine Funktion, z. B. durch Obsoleszenz-Management oder den Wunsch nach einer zusätzlichen Funktion in Ersatzteilen, so handelt es sich um eine wesentliche Änderung im Sinne des CRA. Dessen Auswirkung wiederum ist zu bewerten, und bei Bedarf sind entsprechende Gegenmaßnahmen zu ergreifen. Die sukzessive Angleichung von Ersatzteilen – so dies mit den Zulassungen vereinbar ist – auf CRA-konforme Plattformen stellt somit auch einen wesentlichen Wettbewerbsvorteil dar und reduziert später Aufwände.

3.5 Tailor-made Products

Werden Produkte auf Basis von Kundenspezifikationen hergestellt, so nennt man diese maßgeschneidert. Für maßgeschneiderte Produkte erlaubt der CRA genau zwei Abweichungen von den Anforderungen:
- Sicherheitsupdates müssen nicht mehr kostenfrei zur Verfügung gestellt werden
- Eine Auslieferung ohne sichere Default-Konfiguration, d. h. eine Werkseinstellung mit sicherer (secure) Konfiguration, ist nicht erforderlich.

Der Status maßgeschneidert muss bilateral im b2b abgestimmt werden. Es ist auch denkbar, dass nur ein Teil eines Produktes als maßgeschneidert definiert wird, da eine Anwendung innerhalb des Standard-Produkts angepasst wird.

3.6 Kompatible Systemerweiterungen

Die Erweiterung von Bestandssystemen, egal ob bei Fahrzeugen oder der Infrastruktur, ist ein wesentliches Thema. Der CRA erlaubt die kompatible Systemerweiterung unter Nutzung alter, nicht CRA-konformer Schnittstellen. Damit soll eben sichergestellt werden, dass die Lieferung neuer Produkte keine Rückwirkung auf den Bestand hat, der nicht CRA-konform sein muss. Unter dem Stichwort „Interoperabilität" wird im Erwägungsgrund 55 darauf eingegangen.

Im Gegenzug kann daraus jedoch nicht abgeleitet werden, dass die alte Technik identisch weiter gebaut werden darf. Das neue Produkt muss CRA-konform sein, hat jedoch an der Schnittstelle zum Bestand die begründete Erlaubnis zur Abweichung von den Anforderungen.

Betrachtet man diesen Sachverhalt aus Betreiber und Herstellersicht, erlaubt er eine sukzessive Verbesserung der Cybersecurity unter Schutz des Bestands.

Market launches onto the market are characterised by:
- a physical presence, i.e. the product has been manufactured and has a unique identification number.
- an offer in the market, i.e. in the form of a catalogue or a specific offer to a customer (B2B).

Each individual component is a product. This means that each individually manufactured entity of the same type is placed on the market. The fact that this happens according to the same specification or an existing approval or authorisation is not relevant in terms of the CRA. It is therefore correct that a product that is identical in terms of its technical design can be placed on the market in a non-CRA compliant manner on 10 December 2027, but that CRA compliance will be required on 11 December 2027.

3.4 Spare parts

Spare parts are generally exempt from the CRA, provided they are identical or functionally equivalent. Newly developed spare parts with additional functions, on the other hand, require CRA compliance.

Nevertheless, it is advisable to consider CRA-compliant spare parts at an early stage. This is because any functional changes occurring during the lifecycle, e.g. due to obsolescence management or the desire for an additional function in the spare parts, constitutes a significant change under the provisions of the CRA. The impact of this change must then be assessed and, if necessary, appropriate countermeasures must be taken. The gradual adaptation of spare parts (provided doing so is compatible with the approvals) to CRA-compliant platforms therefore also represents a significant competitive advantage and reduces costs later on.

3.5 Tailor-made products

Products manufactured on the basis of customer specifications are referred to as tailor-made. The CRA allows exactly two deviations from the requirements for tailor-made products:
- security updates no longer have to be provided free of charge
- delivery without a secure default configuration, i.e. a factory setting with a secure configuration, is not required.

The tailor-made status must be agreed bilaterally in b2b. It is also conceivable that only part of a product is defined as tailor-made, because an application within the standard product has been customised.

3.6 Compatible system extensions

The expansion of existing systems, whether in vehicles or infrastructure, is an important issue. The CRA allows compatible system extensions using old, non-CRA-compliant interfaces. This is to ensure that the delivery of new products has no retroactive effect on existing systems, which do not have to be CRA-compliant. This is addressed in recital 55 under the heading "Interoperability".

However, this cannot be taken to mean that old technology may continue to be built identically. The new product must be CRA-compliant, but has justified permission to deviate from the requirements at the interface with the existing system.

From the perspective of operators and manufacturers, this allows for the gradual improvement of cybersecurity, while protecting their existing equipment.

3.7 Implementation with conflict resolution

Ultimately, however, the key question regarding the application of CRA remains as follows: organisational measures can be es-

3.7 Umsetzung mit Zielkonfliktlösung

Die wesentliche Frage zur Anwendung des CRA bleibt am Ende jedoch: Organisatorische Maßnahmen können parallel im Unternehmen aufgebaut werden, doch wie setze ich in bereits genehmigten Produktserien nun die technischen Anforderungen des CRA um?

Der CRA fordert eine risikobasierte Anwendung der Security-Maßnahmen. Diese Risikobewertung soll den geplanten Einsatzzweck berücksichtigen. Des Weiteren ist es erlaubt, Anwendungsbedingungen zu definieren. Dies können z. B. Anforderungen an physische Security, Schulungen von Mitarbeitern, Hintergrundüberprüfungen oder vieles mehr sein. Das verbleibende Restrisiko ist ebenfalls anzugeben. All diese Informationen werden in der Konformitätserklärung angegeben. Kauft ein Kunde ein Produkt, so akzeptiert er diese Bedingungen. Sind diese Bedingungen nicht akzeptabel, wird er es nicht kaufen.

Ergibt sich also eine logische Abfolge aus Komponente (PDE), System (PDE) und Anwendungsumgebung (Betreiber) und sind für alle Teilnehmer die aufgezeigten Restrisiken und Anwendungsbedingungen, wie z. B. kompensierenden Maßnahmen, akzeptabel, so kann CRA-konform die Bereitstellung auf dem Markt erfolgen.

D. h., es existiert eine Brücke für eine sukzessive Verbesserung der Cybersecurity, die einen Übergang erlaubt. Dies kann durch eine gegenseitige Vereinbarung über die Annahme der Anwendungs-

tablished in parallel within the company, but how can the CRA technical requirements be implemented in already approved product series?

The CRA requires the risk-based application of security measures. This risk assessment should take into account the intended use. Furthermore, it is permissible to define the conditions of use. These can include, for example, physical security requirements, employee training, background checks and much more. The remaining residual risk must also be specified. All this information is provided in the declaration of conformity. A customer will accept these conditions when purchasing a product. If, however, these conditions are unacceptable, the customer will simply not purchase the product.

If there is a logical sequence of components (PDE), system (PDE) and application environment (operator) and if the residual risks and application conditions, such as compensatory measures, are acceptable to all the participants, the product can be placed on the market in a CRA-compliant manner.

This means that there is a bridge for the gradual improvement of cybersecurity, allowing for a transition. This may be supported by an agreement about the acceptance of application conditions before placing the product on the market.

However, since NIS2 requires both operators and manufacturers to implement a minimum level of security in their systems, e.g.

bedingungen vor dem Inverkehrbringen des Produkts unterstützt werden.
Aber da NIS2 sowohl Betreiber wie auch Hersteller gleichermaßen auffordert, ein Mindestmaß an Security in ihren Anlagen umzusetzen, z. B. die automatische Detektion von Security-Vorfällen, kann nicht von einem „Weiter so" die Rede sein.
Die genaue Geschwindigkeit der Verbesserung der Cybersecurity ist also – zu einem gewissen Anteil – eine Frage der Risikoakzeptanz. Für Zulieferer und Eisenbahnunternehmen ist es sehr empfehlenswert, schnell auf eine angemessene Anwendung von CRA umzusteigen, um die Risiken der Unternehmen angemessen zu steuern.
Auf dem Bahnmarkt können aktuell verschiedene Strategien beobachtet werden. Es existieren bereits Hersteller, die zum 11. Dezember 2027 ausschließlich neue Produktlinien mit einem hohen Maß an umgesetzten CRA-Maßnahmen anbieten wollen. An anderen Stellen ist noch keine Bewegung zu beobachten.

3.8 Empfehlung

Der CRA gibt glücklicherweise kaum konkrete Anforderungen vor. Weder die technischen Maßnahmen sind spezifiziert, noch die Prozesse definiert. So kann im Bereich des Bahnsektors die ohnehin bereits weithin herangezogene IEC 62443 zur Anwendung kommen. Die Umsetzung der IEC 62443-4-2 auf Komponenten-Ebene und Anwendung der IEC 62443-3-2 für Risikomanagement sowie IEC 62443-4-1 für die sichere (secure) Entwicklung, erfüllen bereits nahezu vollständig die Anforderungen des CRA. D. h., die Ergebnisse können für die Erstellung der Konformitätserklärung genutzt werden. Die ERJU System Pillar Security Specifications, EULYNX Security Requirements und viele weitere Spezifikationen basieren ebenfalls auf der IEC 62443.
Es ist daher stark zu empfehlen, Entwicklungsbemühungen nicht allein auf den CRA auszurichten, sondern die IEC 62443 als Framework heranzuziehen.

4 Fazit

Der CRA markiert für den Bahnsektor einen Paradigmenwechsel. Cybersicherheit wird von einer freiwilligen Zusatzaufgabe oder „nur" Kundenanforderung zu einer verbindlichen regulatorischen Pflicht. Für Hersteller bedeutet dies, Prozesse, Dokumentation und Produktentwicklung daran anzupassen. Für Betreiber wird die Rolle des aktiven Risikomanagers gestärkt, der Restrisiken akzeptieren, dokumentieren und in den Betrieb integrieren muss. Damit entscheidet er maßgeblich über das zu erreichende Security-Niveau.
Die Herausforderung liegt in der Übersetzung der horizontalen Gesetzgebung in sektorale Praxis. Mit den Leitlinien der CSRG und des VDB CIS werden erste Grundlagen bis Ende des Jahres vorliegen, die auch laufende Projekte, Systemerweiterungen und Ersatzteilmanagement berücksichtigen.
Gelingt diese Umsetzung, wird der Bahnsektor nicht nur sicherer, sondern auch zum Vorbild für andere Kritische Infrastrukturen. Er zeigt, wie Security, Sicherheit, Langfristigkeit und Interoperabilität in Einklang gebracht werden können – ein entscheidender Beitrag zur digitalen Souveränität Europas. ■

automatic security incident detection, there can be no question of "business as usual".
The exact speed of cybersecurity improvement is therefore, to a certain extent, a question of risk acceptance. For suppliers and railways, a quick move towards the appropriate application of CRA is highly recommended so as to manage the companies' risks appropriately.
Various strategies can currently be observed in the railway market. There are already manufacturers who want to offer exclusively new product lines with a high level of implemented CRA measures by 11 December 2027. In other areas, no movement can yet be observed.

3.8 Recommendations

Fortunately, the CRA does not specify any concrete requirements. Neither the technical measures nor the processes have yet been defined. This means that IEC 62443, which is already in wide use in the railway sector, can be applied. The implementation of IEC 62443-4-2 at the component level and the application of IEC 62443-3-2 for risk management and IEC 62443-4-1 for secure development already meet the requirements of the CRA almost entirely. This means that the results can be used to prepare the declaration of conformity. The ERJU System Pillar Security Specifications, EULYNX Security Requirements and many other specifications are also based on IEC 62443.
It is therefore strongly recommended that development efforts should not focus solely on the CRA, but that IEC 62443 should be used as a framework.

4 Conclusion

The CRA marks a paradigm shift for the railway sector. Cybersecurity is changing from a voluntary additional task or a "mere" customer requirement to a binding regulatory obligation. For manufacturers, this means adapting processes, documentation and product development accordingly. For operators, the role of the active risk manager, who must accept, document and integrate residual risks into operations, has been strengthened. As such, this individual will play a decisive role in determining the level of security to be achieved.
The challenge lies in translating the horizontal legislation into sectoral practice. The CSRG and VDB CIS guidelines will see the first foundations in place by the end of the year, which will also take into account ongoing projects, system expansions and spare part management.
If this implementation is successful, the rail sector will not only become more secure, but it will also serve as a model for other critical infrastructures that demonstrates how safety, sustainability and interoperability can be reconciled, i.e. a decisive contribution to Europe's digital sovereignty. ■

AUTOR | AUTHOR

Dr.-Ing. Martin Koop
Principal IT / OT Security Expert
INCYDE GmbH
Anschrift / *Address*: Rheinstraße 16a, D-64283 Darmstadt
E-Mail: martin.koop@incyde.com