Cybersecurity – was verlangen die Regularien?

Überblick zu Richtlinien und Verordnungen

TÜV Rheinland Industrie Service GmbH
Joerg Krämer

Veranstaltung:
mobile 2025 ExperienceDays by ifm
im COREUM in Stockstadt a.R.
24. bis 25. September 2025, 9:10 - 9:55 Uhr

TÜVRheinland®
Genau. Richtig.


HOLDER
STOLL
HOLDER



- Wie konnte es dazu kommen?

Selbst fotografiert: Joerg Krämer

Ein kleines Beispiel

Straßenfahrzeug → R155, ISO 21434

Funkverbindung zur Hersteller-Cloud

Wird in der EU auf den Markt gebracht → CRA

Maschinenanbauten → Maschinenverordnung



Selbst fotografiert: Joerg Krämer

TÜVRheinland®
Genau. Richtig.

R155

Gültig ab 07/2024: für alle Neufahrzeuge verpflichtend

Einheitliche Vorschriften über die Genehmigung von Fahrzeugen hinsichtlich ihrer Cyber-Sicherheit und des Cyber-Sicherheitsmanagement-Systems“

- **Für:** HW und SW, Sicherheitsrelevante SW sowie sicherheitsrelevante Komponenten und Maschinen mit KI
- **Inhalt:** Sicherheitsbauteile mit HW/SW ohne Parametrier- oder SW-Updatemöglichkeit

  Gültig: gilt für Pkw, Lkw, Busse und andere Fahrzeuge sowie deren Hersteller, Zulieferer und Zulassungsbehörden z.B.:
  - M: Kraftfahrzeuge zur Personenbeförderung mit mindestens 4 Rädern,
  - N: Fahrzeuge zur Güterbeförderung mit mindestens 4 Rädern,
  - O: Anhänger mit mindestens einem elektronischen Steuergerät

  → Die Regelung fordert die Implementierung eines zertifizierten Cybersecurity Management Systems (CSMS), das lebenslange Schutz vor Cyberbedrohungen gewährleistet.
  → Hersteller müssen Risiken analysieren, Sicherheitsmaßnahmen implementieren und diese nachweislich überwachen und verbessern.

- **Harmonisierte Standards:** Derzeit gibt es keine. Aber es gibt die generische Norm ISO/SAE 21434

TÜVRheinland®
Genau. Richtig.

Ein kleines Beispiel

Straßenfahrzeug → R155, ISO 21434

Funkverbindung zur Hersteller-Cloud → RED

Wird in der EU auf den Markt gebracht → CRA

Maschinenanbauten → Maschinenverordnung



Selbst fotografiert: Joerg Krämer

TÜVRheinland®
Genau. Richtig.

Radio Equipment Directive (RED)

Gültigkeit ab 08/2025



- **Für:** „mit dem Internet verbundene Funkanlagen“ – direkt + indirekt

- **Inhalt:**
  RED ist nicht neu, Erweiterung hinsichtlich Cybersecurity in Artikel 3.3:
  - (d) – Schutz des Netzes und der Dienste
  - (e) – Schutz von personenbezogenen Daten
  - (f) – Schutz vor Betrug

  → Security-Updates über gesamten Produktlebenszyklus (min. 5 Jahre)
  → Meldepflicht für Schwachstellen und Vorfälle

- **Harmonisierter Standard** EN 18031 verfügbar. Die RED wird vermutlich weitgehend von dem CRA abgedeckt werden. Für den CRA ist die IEC 62443 ein guter Weg!

TÜVRheinland®
Genau. Richtig.

Ein kleines Beispiel

Straßenfahrzeug → R155, ISO 21434

Funkverbindung zur Hersteller-Cloud

Wird in der EU auf den Markt gebracht → CRA

Maschinenanbauten → Maschinenverordnung



Selbst fotografiert: Joerg Krämer

TÜVRheinland®
Genau. Richtig.

Cyber Resilience Act (CRA)



Gültigkeiten: 11/2026: Meldepflicht für Schwachstellen/Sicherheitsvorfälle
12/2027: Umsetzung der Anforderungen für neue Produkte

- **Für:** Komponenten mit digitalen Elementen (SW, HW, Remote-Datenverarbeitung)

- **Inhalt:**
  - Annex I: Part I: Essential Cybersecurity Requirements
  - ANNEX I: Part II: Vulnerability Handling Requirements
  - ANNEX II: Information and Instructions to the User
  - ANNEX VII: Contents of the Technical Documentation

In Arbeit:
ISO/CD 24882
Agricultural machinery, tractors, and earth-moving machinery — Cybersecurity Engineering

- **Harmonisierter Standard:** Derzeit keiner! Anwendung der generischen Norm IEC 62443

- **IEC 62443:** etablierter Standard für Cybersecurity in der Industrieautomatisierung
- **Harmonisierter Standard:** Vermutungswirkung zur Erfüllung des Gesetzes → Hersteller kann Selbst-Assessment durchführen
- **Notified Body/Notifizierte Stelle:** Staatlich befugte/überwachte Organisation zur Konformitätsbewertung von Produkten

TÜVRheinland®
Genau. Richtig.

Ein kleines Beispiel

Straßenfahrzeug → R155, ISO 21434

Funkverbindung zur Hersteller-Cloud

Wird in der EU auf den Markt gebracht → CRA

Maschinenanbauten → Maschinenverordnung



Selbst fotografiert: Joerg Krämer

TÜVRheinland®
Genau. Richtig.

Maschinenverordnung (MVo)

Gültigkeit ab 20.01.2027



- **Für:** HW und SW, sicherheitsrelevante SW sowie sicherheitsrelevante Komponenten und Maschinen mit KI
- **Inhalt:**
  - A: Sicherheitsbauteile mit HW/SW ohne Parametrier- oder SW-Updatemöglichkeit
  - B: Sicherheitsbauteile mit Parametrierinterface oder SW-Update-Schnittstelle
  - C: Sicherheitsbauteile mit permanent angeschlossenem Daten-Interface
    (unabhängig ob für Sicherheitsfunktionen verwendet, oder nicht)

    → Maschinen und Steuerungen müssen vor Hackerangriffen geschützt werden
    → Nachweispflicht über Softwareangriffe und Softwareveränderungen

- **Harmonisierte Standards?:**
  - FS: ISO 13849 & IEC 62061
  - CS: im Moment keine! Der Draft der EN 50742 erscheint vermutlich Januar 2026. Sie verweist auf IEC 62443.

TÜVRheinland®
Genau. Richtig.

Global standards for global organizations

Core Standards / Regulations

	Cybersecurity					SW Update	Machinery
	IT Infra	Products	Office	Manufacturing	Road Vehicles	R.V. + Infra	Machines
							
	ISO 2700x	pEN …	ISO 2700x	IEC 62443	ISO 21434	ISO 24089	prEN 50742
							
UNECE					UNECE R-155	UNECE R-156	
	NIS2 (EU) 2022/2555	CRA 2022/0272			(EU) 2019/2144	(EU) 2022/2236	(EU) 2023/1230

TÜVRheinland®
Genau. Richtig.

Richtlinie	Harmonisierte /generische Norm zu CS	Gültig ab/ Übergangszeit	Konformitätsbewertung	Fokus
RED	EN 18031-1/-2/-3	Neu ab 08-2025	Modul B + C (EU-TYPE-Prüfung und Konformität mit der Bauart auf der Grundlage einer internen Fertigungskontrolle) - Benannte Stelle + Fertigungskontrolle Modul H (Konformität auf der Grundlage einer umfassenden Qualitätssicherung) - Benannte Stelle	alle Funkgeräte, die selbst über das Internet kommunizieren können, unabhängig davon, ob sie direkt oder über andere Geräte kommunizieren
CRA	Vertrag zwischen EU-Parlament und CENELEC steht. Jetzt werden AG für harmonisierte Normen erstellt Generische Norm: IEC 62443	Dez.2024 bis Dez. 2027	Module B+C, Module H so lange kein harmonisierter Standard verfügbar ist)	Zielgruppe: Produkthersteller Alle Geräte die auf den europäischen Markt gebracht werden. Quasi CE-Zeichen Level
MVo	prEN 50742 : Januar 2026 Generische Norm: IEC 62443	20.01.2027 Keine Übergangszeit		A: Sicherheitsbauteile mit HW/SW ohne Parametrier- oder SW-Updatemöglichkeit B: Sicherheitsbauteile mit Parametrierinterface oder SW-Update-Schnittstelle (keine permanent angeschlossenen Geräte/Netze, nur für zeitweises Engineering) C: Sicherheitsbauteile mit permanent angeschlossenem Daten-Interface (unabhängig ob für Sicherheitsfunktionen verwendet, oder nicht) Gemäß IEC 62443 SL1/SL2
NIS2		2024		Zielgruppe: Anwender- KRITIS >50 Mitarbeiter >10 Mio. Jahresumsatz z.B.: Abfallwirtschaft (Abfallbewirtschaftung) – KRITIS-Sektor „Entsorgung“ (Important) Lebensmittelproduktion, -verarbeitung und -vertrieb – KRITIS-Sektor „Ernährung“ (Essential) Transport (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr) – KRITIS-Sektor „Transport“ (Essential)
C5-Sicherheits-leitlinie	Vom BSI Cloud Computing Compliance Controls Catalogue (C5)	2018		Cloud zielt darauf ab, den Bürgern die Kontrolle über ihre persönlichen Daten zu geben. Überprüfbaren Mindestanforderungen an die Sicherheit im Cloud Computing. Keine konkreten Maßnahmen! U.a.: - Kontrolle und Überwachung von Dienstleistern und Zulieferern - Management von Sicherheitsvorfällen
UN ECE R155	Nicht harmonisiert aber Generische Norm: ISO/SAE 21434	2021		Im Wesentlichen wird von den Herstellern von Fahrzeugen (genauer: Unternehmen die Fahrzeuge in Verkehr bringen) gefordert, dass sie ein Cybersecurity Management System (CSMS) etablieren und für die Typgenehmigung eines neuen Fahrzeugtyps nachweisen, dass dieses CSMS funktioniert. M: Kraftfahrzeuge zur Personenbeförderung mit mindestens 4 Rädern, N: Fahrzeuge zur Güterbeförderung mit mindestens 4 Rädern, O: Anhänger mit mindestens einem elektronischen Steuergerät
UN ECE R156	Nicht harmonisiert aber Generische Norm: ISO/SAE 21434	2021		Anforderungen im Zusammenhang mit Softwareaktualisierung bei Fahrzeugen. Schreibt die Einführung eines SUMS vor. CSMS und SUMS müssen von einer unabhängigen Prüfstelle („Technischer Dienst“, in Deutschland z. B. der TÜV) zertifiziert und alle drei Jahre geprüft werden. Die Prüfstellen werden im jeweiligen Land von einer autorisierten Staatsstelle (in Deutschland das Kraftfahrtbundesamt) benannt.

Fragen?

Dipl.-Ing. Joerg Krämer

Joerg.Kraemer@de.tuv.com

TÜV Rheinland Industrie Service GmbH
Funktional Sicherheit und Cybersecurity
Qualifizierung & Projektkoordination

LEGAL DISCLAIMER

Dieses Dokument ist Eigentum von TÜV Rheinland. Es dient nur zu vertraulichen Informationszwecken für den Empfänger. Weder dieses Dokument noch irgendwelche Informationen oder Daten, die darin enthalten sind, dürfen ohne vorherige schriftliche Zustimmung von TÜV Rheinland zu anderen Zwecken verwendet oder vervielfältigt oder ganz oder teilweise an Dritte weitergegeben werden. Dieses Dokument ist nicht ohne eine mündliche Erklärung (Präsentation) des Inhalts vollständig.

TÜV Rheinland AG

TÜVRheinland®
Genau. Richtig.