TÜVNORD

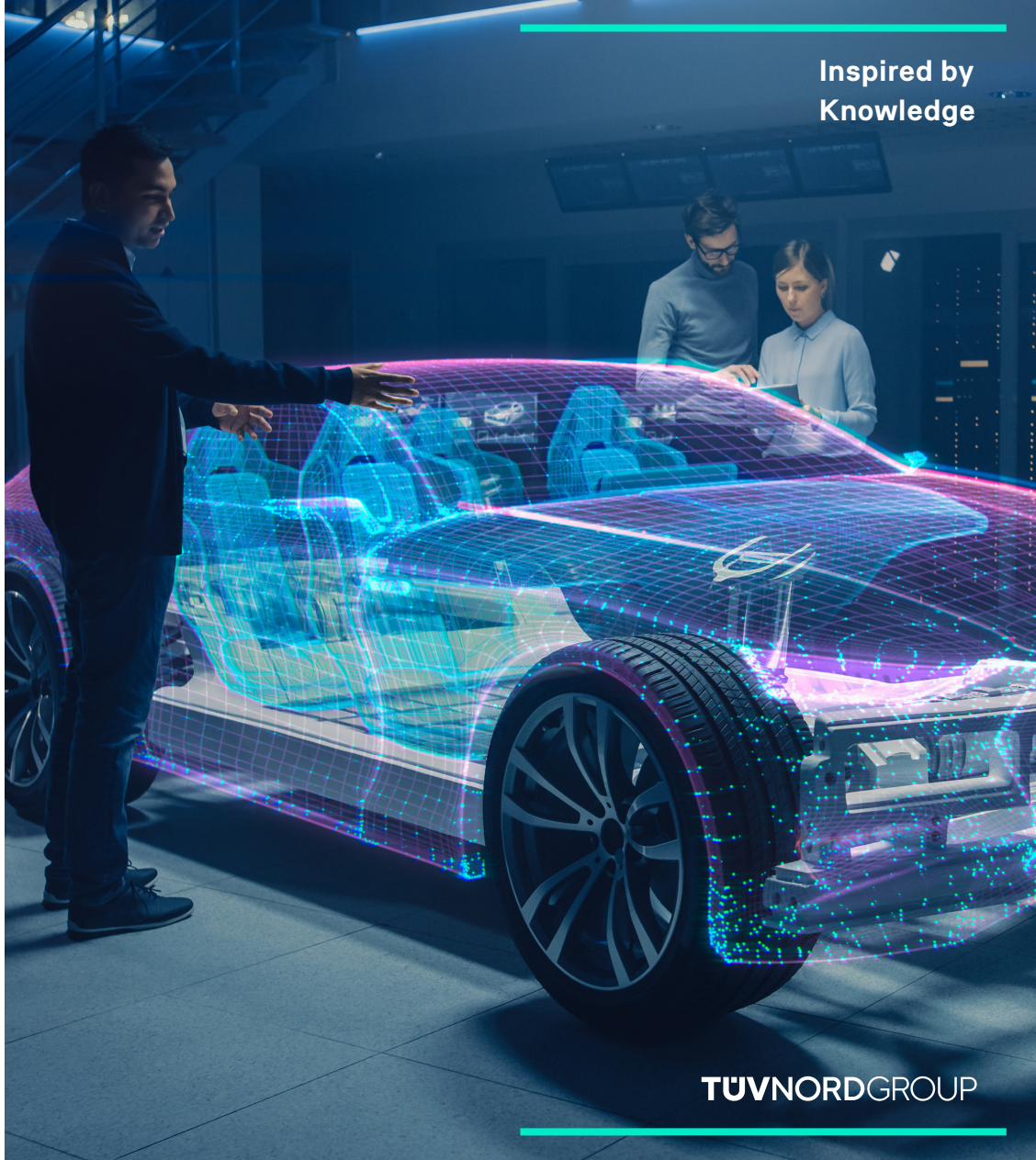
ISO/SAE 21434

Road Vehicles – CSMS Cybersecurity Engineering und Managementsysteme

TÜV NORD CERT

ISMS Sales & Projectmanagement
sales.isms@tuev-nord.de

TÜV®





ISO/SAE 21434
Warum braucht die Automobilindustrie ein CSMS?

Mit der zunehmenden Digitalisierung und Vernetzung im Automobilbereich steigt das Risiko von Cyberangriffen. Zum Schutz der Fahrzeuge und Insassen hat die Wirtschaftskommission für Europa der Vereinten Nationen UNECE die Regelung Nr. 155 (R 155) herausgegeben.

Diese fordert verbindlich, dass Automobilhersteller bei der Zulassung von Serienstraßenfahrzeugen nachweisen müssen, dass sie den Anforderungen an die Cybersicherheit Rechnung tragen. Dazu gehört die Anwendung von Cybersicherheitsmanagementsystemen (CSMS) bei der Entwicklung und Herstellung der Fahrzeuge und der betreffenden Systeme.

Grundsätzlich gilt die Regelung R 155 für alle neuen Fahrzeugtypen,:

- die ab Juli 2022 entwickelt werden, und
- die ab Juli 2024 hergestellt und

in der EU in den Straßenverkehr gebracht werden.

R 155 – Wer ist betroffen und was ist zu tun?

Im Rahmen der R 155 müssen Automobilhersteller unter anderem ermitteln, welche die kritischen Elemente des Fahrzeugs sind und diese einer umfassenden Bewertung auf Cyberrisiken unterziehen. Ferner sind deren Wechselwirkungen zu berücksichtigen und entsprechende Schutzmaßnahmen zu entwickeln – also CSMS. Für die Zulassung der Fahrzeuge sind darüber entsprechende Nachweise vorzulegen.

Warum auch Zulieferer vielfach in der Pflicht sind, den Fahrzeugherstellern Cybersecurity nachzuweisen

Da die Hersteller von Fahrzeugen eine Vielzahl der sicherheitsrelevanten Komponenten und Systemen von spezialisierten Zulieferunternehmen entwickeln und herstellen lassen, werden diese Lieferanten ebenfalls in die Pflicht genommen, die Anwendung eines CSMS nachzuweisen.

Das bedeutet, dass die R 155 zwar in erster Linie die Hersteller betrifft, aber indirekt auch zahlreiche Zulieferunternehmen von kritischen „Items“, wie elektrischen und elektronischen (E/E) Komponenten und Systemen, aber auch Entwickler von IT-Lösungen und sogar Dienstleister von Datenübertragungen.

Um die Anforderungen der R 155 zu erfüllen und dies nachzuweisen, kann die Automobilindustrie auf einen Standard zurückgreifen, der eigens zu diesem Zweck entwickelt wurde: die ISO/SAE 21434 – „Road Vehicles — Cybersecurity Engineering“.

Die ISO/SAE 21434 – „Road Vehicles – Cybersecurity Engineering“

Regulation	UN R 155 (UN R 156)	
Standardisation (Framework)	ISO/SEA 21434 Cybersecurity Engineering	
Standardisation (Audit References)	Automotive SPICE for Cyber-security; Automotive Cybersecurity Management System Audit	ISO PAS 5112
Implementation (3rd Party Audit Scheme)	Own Certification Program (applied for accreditation at DAkkS acc. to ISO/IEC 17021 and ISO/IEC 17065)	TISAX Vehicle Cybersecurity Management

Wofür steht die ISO/SAE 21434 und was fordert sie?



Die ISO/SAE 21434 ist beides, eine Guideline und ein Anforderungskatalog für das Cybersecurity Engineering und Management.

In diesem Sinne soll der Standard dazu beitragen:

- ein einheitliches Verständnis über CSMS und deren Anwendung zu erreichen, unabhängig um welche kritischen Items es geht
- vergleichbare und vor allem wirksame Prozesse und Maßnahmen zu etablieren, um den Cyberrisiken zu begegnen und
- letztlich die erforderliche Transparenz und Nachweisführung zu ermöglichen.

Hauptsächlich geht es bei der ISO/SAE 21434 um die Ermittlung und Bewertung der kritischen Items und ihrer Risiken. Und das über den gesamten Lebenszyklus, von der Entwicklung bis zur Außerbetriebnahme.

Im Zentrum steht dabei die TARA-Methodik (Threat analysis and risk assessment), die die Wirksamkeit des CSMS sicherstellen soll.

Welche Rolle spielen Informationssicherheitsmanagementsysteme (ISMS)?

Für ein wirksames CSMS ist es wichtig, dass eine Organisation ihre Informationen vor unbefugtem Zugriff schützt. Deshalb fordert die ISO/SAE 21434 in Kapitel 5.4.6, dass auch ein Informationssicherheitsmanagementsystem (ISMS) betrieben wird.

Ein ISMS gemäß ISO 27001 oder TISAX® kann zum ganzheitlichen Schutz beitragen. Voraussetzung dafür ist, dass der Geltungs- und Anwendungsbereich des ISMS alle Bereiche des Cybersecurity Engineering umfasst.

Wesentliche Kapitel der ISO/SAE 21434

Kap.	Titel
5	Organisatorisches Cybersecurity Management
6	Projektabhängiges Cybersecurity Management
7	Verteilte Cybersecurity-Aktivitäten
8	Kontinuierliche Cybersecurity-Aktivitäten
9	Konzept
10	Produktentwicklung
11	Cybersecurity-Validierung
12	Produktion
13	Betrieb und Wartung
14	Ende des Cybersecurity-Supports und Außerbetriebnahme
15	“Threat analysis and risk assessment” (TARA) methods
A	Zusammenfassung der Cybersecurity-Aktivitäten und der Arbeitsdokumente



Warum eine Zertifizierung?

Eine Zertifizierung nach ISO/SAE 21434 unterstützt Zulieferer und damit auch Fahrzeughersteller dabei, Cybersecurity Engineering und Management durch eine zusätzliche und neutrale Sicht auf Wirksamkeit und Verbesserungspotenziale prüfen zu lassen und einen objektiven Nachweis darüber zu erlangen.

Dabei ergeben sich folgende Vorteile:

- Auditberichte und Zertifikate sind bewährte Instrumente in der Automobilindustrie, um **wirksame Managementsysteme** und **konforme Produkte** nachzuweisen.
- Erfahrene Auditoren bereiten projektspezifische und effektive Prüfprogramme vor und führen effiziente Audits durch. **Dieses spart Zeit und schont die Ressourcen.**
- Vielfach lassen sich **nicht nur Risiken reduzieren**, sondern ggfs. auch Verbesserungspotenziale aufzeigen und **neue Ansätze** finden.
- Unternehmen **vermeiden Folgeschäden sowie -kosten und schützen ihre Reputation.**

Bestätigungen einer unabhängigen Zertifizierungsstelle zeigen, dass der Stand der Technik angewendet wird und Ihre Organisation einer ständigen Überwachung und kontinuierlichen Verbesserung unterliegt. Dies schafft Vertrauen – national wie international.

Was spricht für TÜV NORD?

TÜV NORD ist renommierter Dienstleister für eine Vielzahl nationaler und internationaler Audit- und Zertifizierungsprogramme. Wir sind seit vielen Jahren für ISO 9001, IATF 16949 und ISO 27001 akkreditiert und langjähriger Audit-Provider für TISAX®.

Da die ISO/SAE 21434 keine Zertifizierungsnorm im klassischen Sinne ist, bedarf es zusätzlicher Regelungen, wie dieser Standard zu auditieren und zu zertifizieren ist. TÜV NORD hat hierzu ein eigenes Zertifizierungsprogramm entwickelt und erfolgreich eingeführt.

Das TÜV NORD Zertifizierungsprogramm berücksichtigt auch die Anforderungen der ISO PAS 5112 – „Road vehicles — Guide-lines for auditing cybersecurity engineering“ und ISO 19011 – „Leitfaden zur Auditierung von Managementsystemen“, sowie des VDA Automotive Cybersecurity Management System Audit (Rotband). Um zu erreichen, dass nach den gleichhohen Anforderungen gearbeitet wird wie auf den anderen Zertifizierungsgebieten, haben wir bei der Deutschen Akkreditierungsstelle (DAkkS) in Berlin dafür eine Akkreditierung nach ISO/IEC 17021 und ISO/IEC 17065 beantragt.

So wird sichergestellt, dass:

- die Auditoren entsprechend qualifiziert sind
- die Audits entsprechend gut vorbereitet und durchgeführt werden
- der Prozess bis zum Zertifikat qualitätsgesichert wird

Machen Sie unsere Vorteile zu Ihren – sprechen Sie deshalb mit uns.

Bitte beachten Sie:
Auf Wunsch prüfen wir neben der Auditierung des eigentlichen CSMS spezifische Komponenten, Produkte und Systeme oder auch IT-Lösungen und vergeben zusätzliche Zertifikate.



TÜVNORD

TÜV®

Inspired by
Knowledge

TÜV NORD CERT
Am TÜV 1
45307 Essen

F 0511 9986 69-1900

tuev-nord-cert.de

TÜVNORDGROUP