TÜVNORD

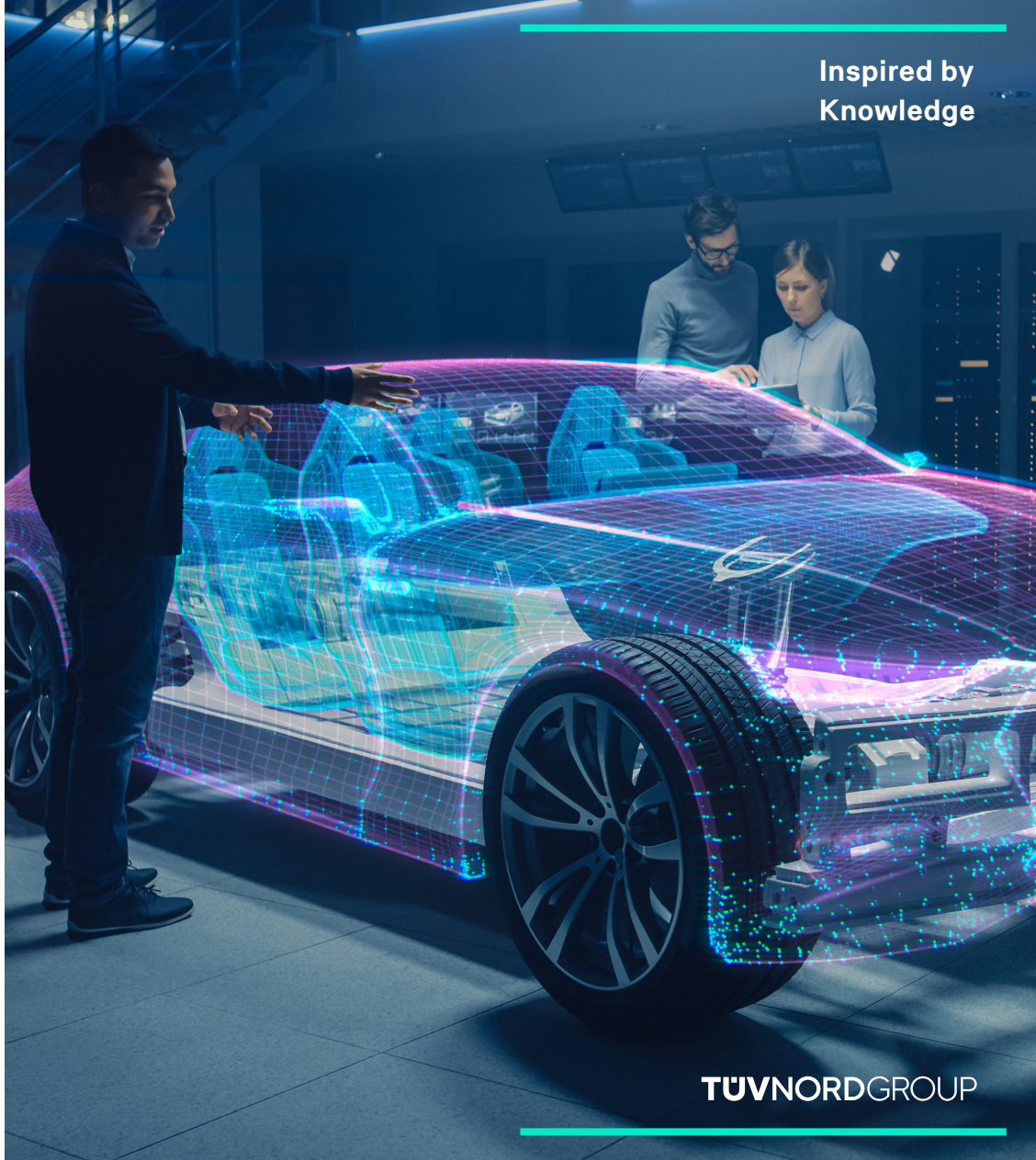
ISO/SAE 21434

Road Vehicles – CSMS Cybersecurity Engineering and Management Systems

TÜV NORD CERT

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

TÜV®



ISO/SAE 21434
Why does the automotive industry need a CSMS?

Greater digitalization and networking in the automotive sector increases the risk of cyber attack. In order to protect vehicles and their occupants, the United Nations Economic Commission for Europe, UNECE, has issued Regulation No. 155 (R 155).

This regulation requires automobile manufacturers to demonstrate fulfilment of extensive requirements for cyber security when applying for type approvals for road vehicles. This includes the use of a cybersecurity management system (CSMS) during development and manufacture of vehicles and cybersecurity-relevant systems.

In principle, Regulation R 155 applies for all new vehicle types which

- were developed in or after July 2022 and
- were manufactured and brought into use on EU roads in or after July 2024.

R 155 – Who is affected and what action is needed?

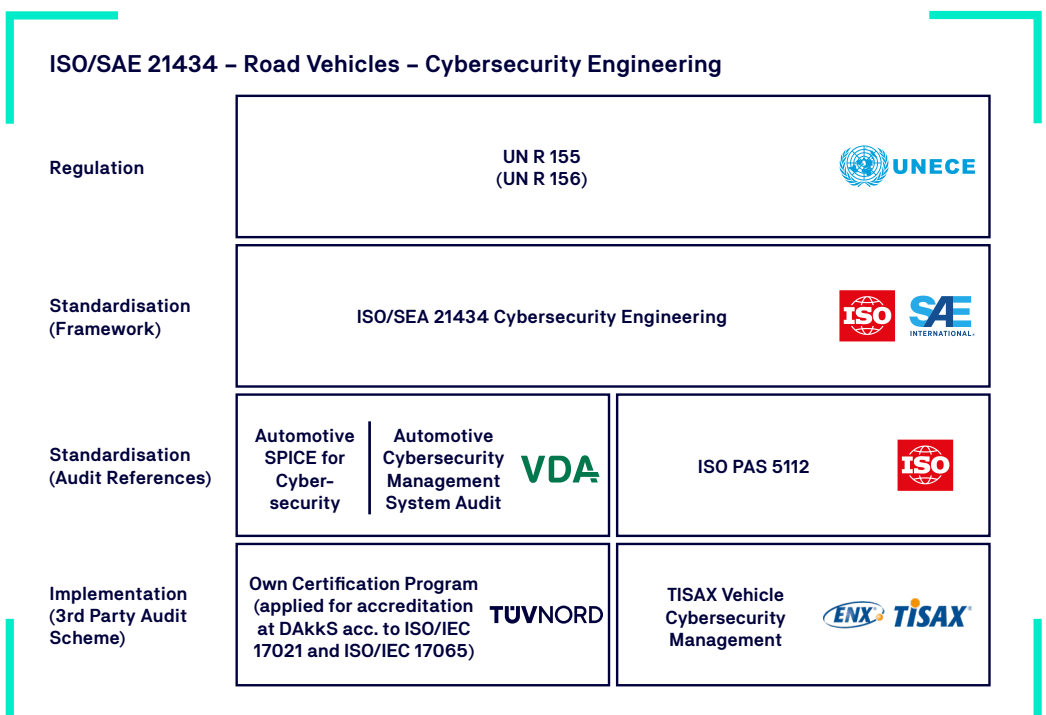
Within R 155 , automobile manufacturers must among other things identify the critical elements of the vehicle and subject them to a comprehensive cyber risk assessment. Interactions between the elements also have to be taken into account and suitable protective measures developed – in other words a CSMS has to be in place.Evidence of this must be provided in order to achieve official vehicle type approval.

Why suppliers are often obliged to demonstrate cybersecurity to vehicle manufacturers

As vehicle manufacturers get a significant number of their security-relevant components and systems developed and manufactured by specialist suppliers, these suppliers also have to demonstrate use of a CSMS.

This means that although R 155 primarily applies to manufacturers, indirectly it also applies to a large number of suppliers of “critical items” such as electrical and electronic (E/E) components and systems, and also to IT solution developers and even data transfer service providers.

In order to demonstrate compliance with R 155, the automotive sector can make use of a standard specifically developed for the purpose: ISO/SAE 21434 – “Road Vehicles — Cybersecurity Engineering”.



What does ISO/SAE 21434 stand for and what are its requirements?

ISO/SAE 21434 is both a guideline and a list of requirements for Cybersecurity Engineering and Management.

The standard is intended to encourage

- consistent and unified understanding of CSMS and their use, independently of particular critical items
- establishment of comparable and above all effective processes and measures in order to counter cyber risks and
- finally, the necessary transparency and provision of suitable evidence.

ISO/SAE 21434 is mainly concerned with the determination and evaluation of critical items and their risks over the entire life cycle, from development down to decommissioning.

The main focus is on “Threat analysis and risk assessment” (TARA) methods, which are intended to ensure the effectiveness of the CSMS.

What role are information security systems (ISMS) playing?

In order for a CSMS to be effective, it is important that the organization protects its information against unauthorised access. Clause 5.4.6 of ISO/SAE 21434 therefore specifies implementation of an information security management system (ISMS).

An ISMS in accordance with ISO 27001 or TISAX® can contribute to comprehensive overall protection. A necessary condition for this is that the scope and area of application of the ISMS covers all aspects of the Cybersecurity Engineering.

Significant clauses of ISO/SAE 21434

Clause	Title
5	Organizational cybersecurity management
6	Project dependent cybersecurity management
7	Distributed cybersecurity activities
8	Continual cybersecurity activities
9	Concept
10	Product development
11	Cybersecurity validation
12	Production
13	Operations and maintenance
14	End of cybersecurity support and decommissioning
15	“Threat analysis and risk assessment” (TARA) methods
A	Summary of cybersecurity activities and work products

Why certification?

Certification to ISO/SAE 21434 supports suppliers and therefore also vehicle manufacturers with audits of Cybersecurity Engineering and Management from an additional and neutral point of view, thus providing the required objective evidence.

Benefits:

- Audit reports and certificates are tried and tested instruments for demonstrating **effective management systems** and **compliant products.**
- Experienced auditors prepare project-specific and effective audit programmes and perform the audits efficiently. **This saves valuable time and resources.**
- Often, it is not only possible to **reduce risks; opportunities for improvement** can also be identified and even **new approaches found.**
- Consequential **damage and costs can be avoided, along with reputational damage.**

Verification by an independent certification body confirms that your systems and technology are state of the art and your organization is subject to constant monitoring and continual improvement. This creates a high level of trust for all stakeholders – both at home and abroad.

Why choose TÜV NORD?

TÜV NORD is a well-known and highly respected service provider for a large number of national and international audit and certification programmes. We have been accredited for ISO 9001, IATF 16949 und ISO 27001 for many years and are a longstanding audit service provider for TISAX®.

As ISO/SAE 21434 is not a certification standard in the traditional sense, additional guidance is needed to show how the necessary audits and certifications must be carried out. TÜV NORD has developed and successfully introduced its own certification programme.

The TÜV NORD certification programme also takes the requirements of ISO PAS 5112 – “Road vehicles — Guidelines for auditing cybersecurity engineering” and ISO 19011 – “Guidelines for auditing management systems”, into account, as well as the VDA Automotive Cybersecurity Management System Audit (Red Volume). In order to ensure that the same high standards apply as to other areas of certification, we have applied for accreditation to ISO/IEC 17021 and ISO/IEC 17065 from the German accreditation body (DAkkS) in Berlin.

This ensures that

- the auditors are suitably qualified
- the audits are well prepared and efficiently carried out
- the process is quality assured right through to the certificate

Benefit from our experience and speak to us.

Please note:
Upon request, besides the auditing of the actual CSMS, we also examine specific components, products and systems and also IT solutions, and issue the relevant additional certificates.

TÜVNORD

Inspired by
Knowledge

TÜV NORD CERT
Am TÜV 1
45307 Essen

F 0511 9986 69-1900

tuev-nord-cert.com

TÜV®

TÜVNORDGROUP