



Add value.
Inspire trust.

Automotive Cybersecurity Management System Assessment

Ensure regulatory and standards compliance

Your challenges

The increasing complexity of connected, automated and autonomous vehicles increases the danger of cyberattacks. To protect vehicles and components, manufacturers must focus beyond the product and create an organisational cybersecurity environment which enables the development of safe and secure products.

The introduction of the UNECE Cybersecurity Regulation will make cybersecurity mandatory for all new vehicles, systems, components and separate technical units. The regulation covers both the cybersecurity of products and the organisational environment. Based on the UNECE regulation, the European Union's General Safety Regulation (GSR) requires cybersecurity for EU type approval.

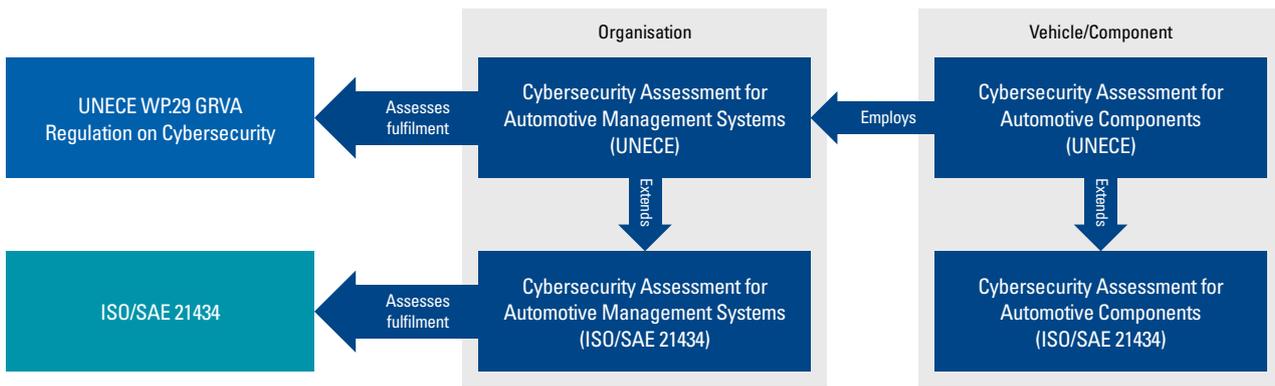
Requirements for automotive manufacturers

The regulation requires automotive manufacturers to maintain a certified "Cybersecurity Management System (CSMS)" which must be assessed and renewed

at least every three years. The CSMS shall ensure that the organisation has the appropriate security measures across the development, production and post-production processes, to produce safe and secure products. The regulation's requirements build upon the upcoming ISO/SAE 21434 standard "Road vehicles - Cybersecurity engineering", which requires an organisational audit. Both the UNECE regulation and ISO/SAE 21434 require cybersecurity to be enforced across the entire automotive supply chain. This will have a significant impact on the automotive industry, including all OEMs, Tier 1 and Tier 2 manufacturers, as well as hardware and software suppliers.

Why is the CSMS assessment important?

Without providing evidence for a CSMS, automotive manufacturers and suppliers cannot gain type approval and will be unable to sell vehicles, components or software in the EU after June 2022. Consequently, Tier 1 and Tier 2 manufacturers, and hardware and software suppliers must give evidence about their capabilities,



including their organisational and engineering cybersecurity processes. With our assessment, you can ensure that you are prepared for the CSMS certification.

How can we help you?

TÜV SÜD’s expert assessment of automotive cybersecurity management systems identifies if your organisation’s processes provide a suitable cybersecurity framework across the product lifecycle, and that you fulfil the CSMS requirements of both the UNECE Cybersecurity Vehicle Regulation and ISO/SAE 21434. With our expert assessment, you can be assured that robust cybersecurity processes exist across your entire organisation.

Our automotive CSMS assessment service

TÜV SÜD experts analyse your organisation’s cybersecurity governance and management. We help you to ensure that project-dependent cybersecurity and engineering processes fulfil UNECE and ISO/SAE 21434 requirements to achieve certification of your CSMS, which can also be provided by TÜV SÜD’s Technical Service. Our detailed technical report includes a performance analysis of each phase and recommends how to close existing gaps.

Our assessments are completely flexible and can be adapted to fit your organisation’s needs, by assessing the entire organisation or covering specific departments. It can also be applied in the early implementation stages and allows for efficient re-assessment, so that changes in your organisation or processes can be reflected quickly.

Your business benefits

- **Reduce business risk** – by ensuring your processes and products fulfil all cybersecurity requirements so that they receive type approval and can be sold on the market.
- **Minimise time to market** – by improving the efficiency of your product development cybersecurity processes.

- **Increase customer trust** – by working with TÜV SÜD’s international network of technical experts and demonstrating your dedication to accurately assessing cybersecurity.

Why choose TÜV SÜD?

TÜV SÜD is an independent third-party service provider with over a century of automotive expertise. Our experts are actively involved in the latest cybersecurity standards development activities (ISO/SAE 21434, ISO PAS 5112 and ISO 24089), providing our clients with the most up-to-date knowledge of current and future requirements. We also participate in relevant UNECE committees to develop regulations on cybersecurity and software updates (UNECE WP.29 GRVA) and have been involved in the development of the first technical guideline in Singapore (TR68-3) for the secure and safe deployment of fully autonomous vehicles. With our systematic and holistic CSMS assessment reports, we enable you to design and verify secure automotive components for connected and automated vehicles.

Add value. Inspire trust.

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specialises in testing, certification, auditing and advisory services. Through more than 25,000 employees across over 1,000 locations, it adds value to its customers, inspiring trust in a physical and digital world.

Related services

- TÜV SÜD provides the following related services:
- Cybersecurity Assessment for Automotive Components & Connected Vehicles
 - Permit for Operating Autonomous Vehicles on Public Roads