Add value.
Inspire trust.

Cybersecurity assessment for automotive components

Ensure your components are robust and resilient

Your challenges

The growing digitisation of vehicle technology is increasing the complexity of modern vehicles today. More and more electronic control units (ECU) are installed in vehicles to implement new innovative functions. However, with the large number of those functions and electrical and electronic (E/E) components the potential risk of cyberattacks is increasing, especially for automated driving functions and autonomous vehicles. Another element of uncertainty lies in the extended supply chain as components often integrate third-party software and hardware. Manufacturers must ensure that all those components are resilient to cyberattacks. Otherwise, this can result in potential operational and financial damage for the manufacturer, and at the same time threaten the data security of vehicle users and safety of road users.

Currently, multiple recommendations and best practices for the cybersecurity of modern vehicle technology exist, but norms and regulations are still under development. Consequently, it is very challenging for manufacturers to be entirely sure if an automotive component has been developed securely and whether it offers suitable cybersecurity protection levels.

Why is cybersecurity for automotive components important?

As a consequence of the increasingly complex technologies used, cybersecurity becomes essential for modern, connected and autonomous vehicles and components.

But it is important that the cybersecurity of vehicle components is not treated in isolation. Instead, it must be holistically assured throughout a manufacturer's entire organisation, as well as across the whole product lifecycle. Component cybersecurity must be ensured from the development process right through to decommissioning, and across the entire manufacturing organisation and its processes.

How can we help you?

TÜV SÜD's cybersecurity assessment for automotive components helps manufacturers to answer these complex challenges by ensuring they develop a robust product that provides suitable cyberattack protection. Our assessment service ensures that:

- Manufacturers implement suitable cybersecurity governance and management
- Appropriate development processes are met over the entire product lifecycle
- The correct technical security measures are developed in line with relevant norms, regulations and recommendations

Our cybersecurity assessment services

TÜV SÜD's comprehensive services cover the full system (both hardware and software), as well as software-only and hardware-only components. Also, off-the-shelf components, i.e. components which are not developed for a specific ECU, can be assessed. We support all phases of the development process, including products at the early design phase. This helps to ensure that robust cybersecurity management exists across the entire organisation, as well as within the product development process, and that it is in line with existing standards, regulations and best practices.

Our TÜV SÜD services include the assessment of:

- All phases of the product lifecycle
- Product-related cybersecurity management across the organisation and for a specific project
- Effectiveness and appropriateness of technical security measures

As a result, you will receive the following deliverables:

- Technical assessment report, highlighting product lifecycle strengths and weaknesses of different phases
- List of critical elements
- Recommendations for improvements

Your business benefits

- **Develop secure automotive components** – which are resilient against cybersecurity threats and meet relevant standards and regulations.
- **Increase business efficiency** – by improving your cybersecurity-related component development processes.
- **Increase customer trust** – by providing secure products and proving that cybersecurity risks have been accurately assessed and well mitigated.
- **Gain a competitive edge** – by working with an independent third-party service provider that has an international expert network and a wealth of automotive and cybersecurity experience.

Why choose TÜV SÜD?

TÜV SÜD is an independent third-party service provider with over a century of automotive safety, security and performance expertise. Our experts are actively involved in the latest cybersecurity standards development activities (ISO/SAE 21434 and ISO 24089), providing our clients with the most up-to-date knowledge of current and future requirements. In addition, our TÜV SÜD experts also participate in relevant UNECE committees to develop regulations on cybersecurity and software updates (UNECE WP.29 GRVA). Furthermore, we 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 assessment of products over your entire product lifecycle, we ensure that our assessment reports 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 24,000 employees across over 1,000 locations, the company adds value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in a physical and digital world to create a safer and more sustainable future.

Related services

TÜV SÜD provides the following related services:

- Permit for operating autonomous vehicles on public roads
- Cybersecurity assessment for connected and automated vehicles

TÜV SÜD AG Westendstr. 199, 80686 Munich, Germany
+49 89 5791-0 automotive@tuvsud.com www.tuvsud.com/automotive