ISO/SAE 21434

ROAD VEHICLES
CYBERSECURITY ENGINEERING

WHAT IS ISO/SAE 21434?

ISO/SAE 21434 is the world's first international standard for cybersecurity in the automotive industry. It aims to reduce the risk of cyberattacks by embedding cybersecurity into automotive products throughout their lifetime.

The standard specifies engineering requirements for cybersecurity risk management. These requirements cover the concept, product development, production, operation, maintenance and decommissioning of series production electrical and electronic (E/E) systems in road vehicles, whose development or modification began after the standard was published in 2021. This includes their components and interfaces. The standard does not prescribe specific cybersecurity technology or solutions.

WHY IS ISO/SAE 21434 IMPORTANT?

The shift toward vehicle connectivity and automated vehicles, coupled with increasing numbers of complex automotive components, has heightened the risk of cyberattacks.

ISO/SAE 21434 provides guidance on developing a cybersecurity management system that includes processes for risk assessment, treatment, monitoring and review. Its framework includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risks.

WHAT WE OFFER?

As the world's leading testing, inspection and certification company, with decades of experience in the automotive and cybersecurity arenas, we can help you along the path to certification with an ISO/SAE 21434 audit. Your audit can include a gap assessment and benchmarking. We will determine your level of competence and provide advice on how to achieve ongoing improvement. We also offer a range of complementary training courses.

WHO IS IT FOR?

Any automotive organization or professional, including risk managers, looking to:

- Reduce the risk of automotive cyberattacks
- Embed cybersecurity into automotive products throughout their lifetime
- Understand the engineering requirements for cybersecurity risk management concerning series production E/E systems

KEY BENEFITS

- Ensure that products and services are developed and maintained in a secure and trustworthy management process
- Better identify and mitigate potential threats and vulnerabilities
- Indicate that you have conducted a security assessment with the greatest possible independence
- Demonstrate your level of embedded cybersecurity to customers
- Improve operational efficiency and reduce costs
- Contribute to UN Sustainable Development Goal 9 – Industry, Innovation and Infrastructure
- Help comply with other relevant standards and regulations, such as UNECE Regulation No. 155 (cybersecurity and cybersecurity management system) and the General Data Protection Regulation (GDPR)

A STEP-BY-STEP CERTIFICATION PROCESS

1. Understand the standard – learn about the requirements
2. Get in touch – tell us what standard you are aiming for, and we will provide a detailed proposal and quote
3. Competence – we will identify any skill and competence gaps that your staff may have. We can provide training and workshops to support you
4. Gap assessment – we will identify any weaknesses
5. Stage 1 – confirmation that implementation of the standard is on track
6. Stage 2 – confirmation that the standard is fully implemented
7. Certification – we will issue your certificate, outlining the scope. Once you are certified, you can share your achievement with the world. Your stakeholders can check your certification via our Client Directory
8. Ongoing improvement – regular surveillance visits to help you maintain and enhance your management system

ABOUT SGS

We are the world's leading testing, inspection and certification company. We are recognized as the global benchmark for sustainability, quality and integrity.

For more information on our ISO/SAE 21434 services, email: certification@sgs.com.

SGS.COM

SGS