Automotive Security & Safety

The automotive industry is facing new challenges as a result of increasing digitalization and networking, the introduction of automated driving and shared mobility as well as changing value chains. While this presents many opportunities, it unfortunately also increases exposure to cybersecurity threats and attacks. To meet these challenges, ever-increasing demands on cybersecurity have to be taken into account, something that is also reflected in the growing number of statutory regulations in this area and the defined deployment dates, such as UNECE Regulation 155 for the EU or the GB44495 standard for China. Implementation will be staggered: For new vehicle types, for example, July 1, 2022, in accordance with UNECE Regulation No. 155 and January 1, 2026, in accordance with the Chinese standard GB 44495-2024 are the deadlines. For the new registration of already type-approved vehicle types, July 1, 2024, applies in accordance with the UNECE regulation and January 1, 2028, in accordance with GB 44495-2028.

To ensure the best possible protection for vehicles against cyber attacks and to provide traceable software updates, AUDI AG has implemented an Automotive Security Management System (ASMS) to fulfill the relevant statutory requirements. The ASMS encompasses both a Cyber Security Management System (CSMS) and a Software Update Management System (SUMS). In addition to compliance with the statutory requirements, the provisions of ISO/SAE standard 21434 were taken into account when designing the CSMS. This standard defines requirements for cybersecurity risk management for electric and electronic systems in road vehicles.

The CSMS aims to monitor and control the cybersecurity of vehicles and vehicle-related IT systems according to risk. The defined objectives of the CSMS are implemented on the basis of policies, processes and control measures. Before production commences, the vehicles are developed in line with the security-by-design principle, taking account of identifiable threats. This ensures that the vehicle and its onboard electronics are protected against unauthorized access.

Once production commences, the cybersecurity of vehicles in the field and vehicle-related IT systems is monitored and appropriate corrective actions, e.g. software updates, are taken if necessary.

Periodic audits are conducted by technical services on behalf of the authorities to ensure that the requirements arising from the underlying statutory regulations are correctly implemented for the CSMS. UNECE Regulation 155 stipulates a three-year interval for recertification with additional annual audits. Certificates are issued based on the results of these audits. For example, AUDI AG was first certified in 2021 by the Société Nationale de Certification et d'Homologation (SNCH) for the UNECE region or in 2024 by the China Quality Certification Centre (CQC) for China or by the South Korean Ministry of Land, Infrastructure and Transport (MOLIT) in 2025. Further audits and certifications, including for India and Taiwan, will follow.

The statutory regulations referred to not only describe requirements for the CSMS and its processes, but also requirements for vehicle types, compliance with which is to be demonstrated as part of the type approval process.

The following aspects have been implemented in this regard:

- Procedures for identifying and evaluating cybersecurity threats and risks in vehicles and their ecosystem, including consideration of suppliers and other development partners
- Procedures for avoiding and/or handling identified cybersecurity threats and risks
- Procedures for monitoring products in relation to cybersecurity attacks and new cybersecurity threats

Ingolstadt, February 2026

- Procedures for maintaining or restoring cybersecurity
- Adaptation of the homologation process for presenting a valid certificate for the management system (if applicable)

Corresponding procedures, roles and methods are established and enhanced continually so that the statutory requirements for a CSMS can be fulfilled and customers protected.

Functional safety

In addition to the cybersecurity of the vehicle, other aspects of product safety are considered and implemented.
Functional safety is implemented according to the requirements of ISO 26262 for all vehicles. This standard describes
requirements for the functional safety of electric or electronic vehicle systems. The objective is to protect people and the
environment from the consequences of these systems malfunctioning.

In addition, the Safety of the Intended Functionality (SOTIF) according to ISO 21448 is evaluated for functions relating to driver assist systems and conditional automation. This standard describes the safety of the target function, with the aim of protecting people and the environment from unreasonable risks posed by these functions.
Our vehicles are systematically analyzed, developed (safety-by-design) and manufactured on the basis of these standards.

Key aspects of the approach include:
- Identification of potential hazards
- Evaluation of the risks associated with these hazards
- Implementation of suitable safety measures to avoid or mitigate these risks

Compliance with the requirements set out in the standards is documented and is subject to regular internal and external
audits. As part of a certification audit, the technical service ATEEL S.à r.l. confirmed the compliance of the development
process at AUDI AG with the requirements of ISO 26262.

We make it a top priority to ensure the safety of our products and therefore the protection of our customers. On the basis of UNECE Regulation No. 171 for driver assist systems, AUDI AG has defined and implemented a comprehensive safety management system. The correct implementation of the requirements for this management system has been confirmed by the independent technical service ATEEL S.à r.l. during an external audit.

Ingolstadt, February 2026