Automotive security & safety

The automotive industry is facing new challenges. With increasing digitalization – for example, connectivity, automated driving and shared mobility – the value chain is changing and providing a wide range of opportunities for cyberthreats. The requirements of cybersecurity are also continuously on the rise within this context.

AUDI AG has implemented an Automotive Security Management System (ASMS) to protect vehicles from cyberthreats and to provide secure and traceable software updates. This system is divided into the Cybersecurity Management System (CSMS) and the Software Update Management System (SUMS).

The goal of the CSMS is to minimize cybersecurity risks to vehicles throughout their entire life cycle. To this end, the CSMS uses guidelines and standards to describe what is necessary to manage the cybersecurity risks to vehicles.

By issuing a certificate to AUDI AG, the authority Société Nationale de Certification et d'Homologation (SNCH) confirmed the effectiveness of the Group's CSMS. This was preceded by a certification audit during which the technical service ATEEL audited the CSMS at AUDI AG in accordance with the requirements of UNECE Regulation No. 155. The certificate is valid for three years and is reviewed as part of an annual monitoring audit.

Among others, the following aspects are part of the considerations:

- Procedure to identify and assess cybersecurity risks to vehicles and their ecosystem
- Procedure for dealing with the cybersecurity risks that are identified

Corresponding procedures, roles and methods have been established at AUDI AG and are continuously evolved to ensure compliance with the requirements of a CSMS pursuant to UNECE Regulation No. 155.

Functional safety

In addition to cybersecurity, functional safety is also implemented in the vehicle electronics.

Audi assesses the topic pursuant to ISO 26262 – a global standard for functional safety in the automotive industry. This standard describes the requirements for design, development and validation of electronic vehicle systems with the goal of protecting people or the environment against malfunctions of electronic vehicle systems. ISO 26262 forms the foundation for analyzing and developing our vehicles with a systematic approach to safety.

Core parts of the process are:
- Identification of potential hazards
- Assessment of the risks associated with these hazards
- Implementation of suitable safety measures to reduce these risks

The safety of our products – and thus the protection of our customers – is one of our top priorities.