Automotive Security & Safety

Die fortschreitende Digitalisierung und Vernetzung, die Einführung des automatisierten Fahrens sowie Shared Mobility und veränderte Wertschöpfungsketten stellen die Automobilbranche vor neue Herausforderungen. Dadurch eröffnen sich zahlreiche Möglichkeiten – leider auch für Cyberbedrohungen und -angriffe. Um diesen gewachsen zu sein, müssen stetig steigende Anforderungen an die Cyber Security berücksichtigt werden, was sich auch durch die steigende Zahl der dazu geschaffenen gesetzlichen Regelungen und den definierten Einsatzterminen ausdrückt, wie z. B. der UNECE-Regelung 155 für die EU oder dem Standard GB44495 für China. Die Umsetzung erfolgt gestaffelt: Für neue Fahrzeugtypen gelten beispielsweise der 1. Juli 2022 gemäß UNECE-Regelung Nr. 155 sowie der 1. Januar 2026 gemäß der chinesischen Norm GB 44495-2024 als Stichtage. Für die Neuzulassung bereits typgenehmigter Fahrzeugtypen gelten entsprechend der UNECE-Regelung der 1. Juli 2024 und gemäß GB 44495-2024 der 1. Januar 2028.

Um Fahrzeuge vor Cyberangriffen bestmöglich zu schützen und nachvollziehbare Software-Updates bereitzustellen, hat die AUDI AG zur Erfüllung einschlägiger gesetzlicher Vorgaben ein Automotive Security Management System (ASMS) implementiert. Dieses umfasst sowohl ein Cyber Security Management System (CSMS) als auch ein Software Update Management System (SUMS). Für die Ausgestaltung des CSMS wurden neben den gesetzlichen Anforderungen auch die Vorgaben der ISO/SAE-Norm 21434 beachtet. Diese Norm legt Anforderungen an das Cyber Security-Risikomanagement für elektrische und elektronische Systeme in Straßenfahrzeugen fest.

Das CSMS zielt darauf ab, die Cyber Security von Fahrzeugen und fahrzeugnahen IT-Systemen risikobasiert zu steuern, zu kontrollieren und zu überwachen. Die Umsetzung der definierten Ziele des CSMS erfolgt auf Basis von Richtlinien, Prozessen und Kontrollmaßnahmen. Die Fahrzeuge werden vor Produktionsstart nach dem Security-by-Design-Prinzip unter Berücksichtigung erkennbarer Bedrohungen entwickelt. Dadurch werden das Fahrzeug und dessen Bordelektronik gegen unberechtigte Zugriffe geschützt. Nach Produktionsstart wird die Cyber Security der Fahrzeuge im Feld sowie der fahrzeugnahen IT-Systeme überwacht, und bei Bedarf werden geeignete Maßnahmen, wie z.B. Softwareupdates, ergriffen.

Die korrekte Umsetzung der Anforderungen aus den zu Grunde liegenden gesetzlichen Regelungen für das CSMS wird in wiederkehrenden Audits von technischen Diensten im Auftrag der Behörden festgestellt. In der UNECE-Regelung 155 ist dieses im Abstand von 3 Jahren für die Rezertifizierung mit ergänzenden jährlichen Prüfungen festgelegt. Die Ergebnisse sind die Basis für die Zertifikaterteilung, wie sie für die AUDI AG z. B. durch die Société Nationale de Certification et d'Homologation (SNCH) für den UNECE-Raum erstmals 2021 oder durch das China Quality Certification Centre (CQC) für China in 2024 erfolgt ist. Weitere Audits und Zertifizierungen u. a. für Südkorea oder Taiwan werden folgen.

Die genannten gesetzlichen Regelungen beschreiben nicht nur Anforderungen an das CSMS und dessen Prozesse, sondern auch Anforderungen an die Fahrzeugtypen, deren Erfüllung im Rahmen der Typgenehmigung nachzuweisen ist.

Hierzu wurden folgende Aspekte umgesetzt:

- Verfahren zur Identifizierung und Bewertung von Cyber-Security-Bedrohungen und -Risiken der Fahrzeuge und ihres Ökosystems inkl. der Berücksichtigung von Lieferanten und anderen Entwicklungspartnern
- Verfahren zur Vermeidung von und/oder zum Umgang mit den festgestellten Cyber-Security-Bedrohungen bzw. -Risiken
- Verfahren zur Beobachtung der Produkte hinsichtlich Cyber-Security-Angriffen und neuen Cyber-Security-Bedrohungen

- Verfahren zur Aufrechterhaltung oder Wiederherstellung der Cyber Security
- Anpassung der Homologationsverfahren zur Vorlage eines gültigen Zertifikats für das Management-System (wenn anwendbar)

Entsprechende Verfahren, Rollen und Methoden sind etabliert und werden kontinuierlich weiterentwickelt, um die gesetzlichen Anforderungen an ein CSMS zu erfüllen und den Schutz der Kunden zu ermöglichen.

Functional Safety

Zusätzlich zur Cyber Security des Fahrzeugs werden weitere Aspekte der Produktsicherheit berücksichtigt und angewendet.
So wird die funktionale Sicherheit entsprechend den Vorgaben der ISO 26262 für alle Fahrzeuge umgesetzt. Diese Norm beschreibt Anforderungen an die funktionale Sicherheit von elektrischen oder elektronischen Fahrzeugsystemen. Ziel ist es, Menschen und Umwelt vor den Auswirkungen des Fehlverhaltens dieser Systeme zu schützen.

Zusätzlich wird für Fahrerassistenzsysteme und hochautomatisiertes Fahren betreffende Funktionen die Safety of the Intended Functionality (SOTIF) gemäß IS0 21448 bewertet. Diese Norm beschreibt die Sicherheit der Sollfunktion. Ziel ist es, Menschen und Umwelt vor unzumutbaren Risiken durch diese Funktionen zu schützen.
Auf Grundlage dieser Normen werden unsere Fahrzeuge systematisch analysiert, entwickelt (safety-by-design) und gefertigt.

Wesentliche Bestandteile der Vorgehensweisen sind:
- Die Identifikation potenzieller Gefahren
- Die Bewertung der mit diesen Gefahren verbundenen Risiken
- Die Umsetzung geeigneter Sicherheitsmaßnahmen zur Vermeidung oder Minderung dieser Risiken

Die Einhaltung der in den Normen enthaltenen Vorgaben wird dokumentiert und unterliegt regelmäßigen internen und externen Audits. In einem Zertifizierungsaudit hat der Technische Dienst ATEEL mit Erteilung eines Zertifikates die Erfüllung der Anforderungen der ISO26262 an den Entwicklungsprozess für die AUDI AG bestätigt.

Die Sicherheit unserer Produkte und somit der Schutz unserer Kunden gehört zu unseren obersten Prioritäten.