© ETAS

Cybersecurity fürs autonome Fahren

Fahrerlose Angriffsziele

Ab SAE Level 4 entsteht für autonome Fahrzeuge eine neue Risikolage mit höheren Anforderungen an deren Absicherung vor Cyberattacken, unerlaubten Zugriff und Manipulation. Als „Schutzmacht und Ausfallbürgschaft" wird Cybersecurity zur fundamentalen Voraussetzung für das autonome Fahren.

Michael Friedrich und Wolfram Gottschlich

Weltweit zeugen Pilotprojekte davon, dass verlässlich funktionssichere autonome Fahrsysteme an der Schwelle zur technologischen Umsetzung stehen. Das Versprechen: Erhöhte Verkehrssicherheit durch Vermeidung menschlicher Fehler und zugleich eine ganz neue Qualität vernetzter Mobilität. Beim vollautomatisierten Fahren ab SAE Level 4 übernehmen verteilte Systeme in der E/E-Architektur – und potenziell auch außerhalb der Fahrzeuge – die Steuerung des Fahrzeugs ohne einen Fahrer in der Kette. Funktionale Sicherheit und Robustheit der Fahrfunktion basieren allein auf Sensorik und deren Verarbeitung in den Fahrzeugsystemen.

Große Angriffsfläche, hohes Schadenspotenzial

Automotive Cybersecurity, der Schutz der Fahrzeuge vor unerlaubtem Zugriff oder Manipulation und die Absicherung der Verfügbarkeit wichtiger Fahrzeugsysteme erlangt vor diesem Hintergrund fundamentale Bedeutung. Autonome Fahrzeuge werden für Angreifer zu einem attraktiven Ziel – aus zweierlei Gründen: Sie bieten eine große, vielgestaltige Angriffsfläche, und sie bergen hohes Schadenspotenzial.

Tatsächlich nimmt die Zahl potenzieller Angriffsvektoren beim vollautomatisierten Fahrzeug ab SAE Level 4 deutlich zu. Denn die Verwirklichung autonomer Fahrfunktionen geht in aller Regel mit permanenter, hochgradiger Vernetzung einher – zum Beispiel durch den

Abruf von Kartenmaterial, vernetzte Cloud-Services oder V2X-Kommunikation mit anderen Fahrzeugen und Verkehrsinfrastruktur. Darüber hinaus eröffnet die notwendige umfassende Sensorik neuartige Angriffsmöglichkeiten.

Gleichzeitig steigt beim autonomen Fahren das mögliche Ausmaß des durch einen Cyberangriff verursachten Schadens erheblich. Dass sich einzelne Fahrzeugsysteme und -funktionen über Sicherheitslücken aus der Ferne übernehmen lassen, haben Miller/Valasek bereits 2015 demonstriert [1].Fahrerassistenzsysteme geben bei Funktionsstörung die Kontrolle an den Fahrer zurück Kompromittierte oder gar gekaperte Fahrzeugsysteme in einem autonomen Fahrzeug hingegen verfügen nicht mehr über die Rückfallebene in Gestalt des korrigierend eingreifenden Fahrers.

No Safety without Security

Daran zeigt sich: Beim autonomen Fahrzeug bilden die Cybersicherheit (Security) und die funktionale Sicherheit (Safety) der Fahrfunktionen geradezu eine „Schicksalsgemeinschaft", die es intelligent zu managen gilt. So müssen die Safety-relevanten Systeme nicht nur robust gegen Cyberattacken sein, sondern auch Rückfallebenen im Falle einer Teilkompromittierung bieten. Selbst im Fall eines erfolgreichen Angriffs, sollte die Grundfunktionalität der autonomen Systeme aufrechterhalten bleiben, um die funktionale Sicherheit des Fahrzeugs nicht zu gefährden (**Bild 1**).

Die Konvergenz von Security und Safety wird zu einem entscheidenden Faktor: So spielen etwa Cloud-Systeme bei der praktischen Umsetzung autonomer Fahrfunktionen häufig eine wichtige Rolle: Sie ermöglichen u.a., das Fahrzeug an einen bestimmten Ort zu rufen oder starten Parkvorgänge. Zugleich sind sie ein mögliches Einfallstor, über das Angreifer Fahrzeuge kapern und zum Beispiel Verkehrschaos stiften könnten. Sind ebendiese Cloud-Services indes Security-seitig gegen unautorisierten Zugriff abgesichert, können sie über den Fernsteuerungsmechanismus zum wichtigen Bestandteil des Betriebskonzepts der Flotte werden: Sie erlauben einem Operator im Backend, das Fahrzeug aus einer kritischen Situation heraus zu führen – und werden so von einer potenziellen Bedrohung zum möglichen „Rettungsanker".

Neuartige Herausforderungen für die Cybersicherheit

Dass das Fahrzeug die Fahraufgabe über eine gewisse Zeit, in gewissen Situationen oder vollständig selbst übernimmt, setzt zwingend voraus, dass die autonomen Systeme jederzeit verfügbar und funktionsfähig sind. Im Gegensatz zu Fahrerassistenzsystemen müssen autonome Systeme auch die letzte Rückfallstufe zur sicheren Ausführung der Fahrfunktion darstellen. Ihre Absicherung gegen unerlaubten Zugriff und Manipulation muss das mit einbeziehen – Cybersecurity stellt nicht nur die „Schutzmacht" der autonomen Systeme dar, sondern auch deren „Ausfallbürgschaft". Das bringt eine Reihe neuer Herausforderungen mit sich (**Bild 2**):

- Heterogene Rückfallebenen
- Hohe Datenraten
- Adversial Attacks
- Regulatorische Rahmenwerke

Heterogene Rückfallebenen

Zur Resilienz von autonomen Fahrzeugen gehören einerseits der Schutz von Daten innerhalb des Systems, andererseits die verlässliche Umgebungserkennung mittels der Sensorik als unmittelbare Basis für die Fahrentscheidungen. Daten innerhalb des autonomen Systems lassen sich durch klassische IT-Security-Mechanismen wie Verschlüsselung, Integritätsschutz und Authentifikation schützen. Diese klassischen Mechanismen helfen jedoch nicht gegen Angriffe auf die Algorithmen, die mit maschinellem Lernen die sensorische Umfelderfassung umsetzen. Sowohl die Steuerung der Fahrfunktionen als auch die Umgebungserkennung sollten mit Hilfe von Redundanzen heterogene Rückfallebenen schaffen. So ist etwa bei einer Teilkompromittierung Safety-relevanter Fahrsysteme sicherzustellen, dass zumindest deren Grundfunktionalität verfügbar und erhalten bleibt. Ebenso muss die Umgebungserkennung, beispielsweise in der Sensorfusion, feststellen können, wenn ein Teil der Sensordaten nicht plausibel ist: Das Fahrzeug kann dann idealerweise weiterhin sicher fahren, solange eine sensorische Umfelderfassung in ausreichendem Maße erfolgt.

Das Defense-in-Depth-Prinzip, die vielschichtige Absicherung mit spezifischen Schutzmechanismen auf relevanten Systemebenen ist hier also wichtiger denn je, muss aber über die Ebe-

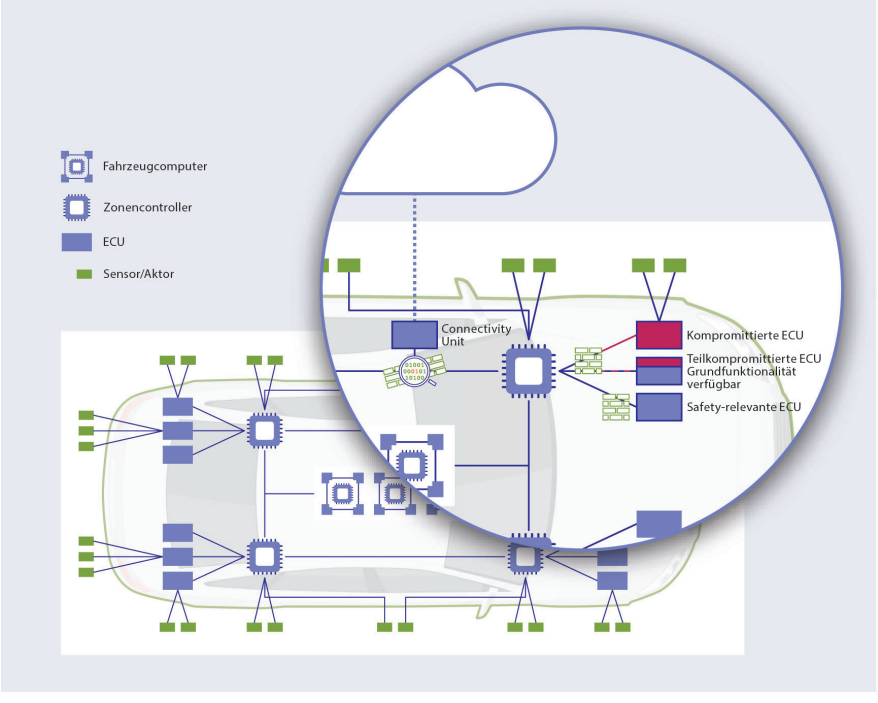

Bild 1: Security-Maßnahmen müssen im autonomen Fahrzeug Rückfallebenen schaffen, über die die Grundfunktionalität (teil-)kompromittierter Safety-relevanter Systeme aufrechterhalten bleiben. © ETAS

nen hinweg die besonderen Implikationen und Notwendigkeiten autonomen Fahrens mit einbeziehen (**Bild 3**).

Hohe Datenraten

Autonome Fahrzeuge werden in Zukunft hohe Datenraten im Gigabit-Bereich in Echtzeit verarbeiten, um Fahrsituationen meistern zu können. Allein bei der Umgebungserkennung durch Kamera, Lidar, Radar oder Ultraschall entstehen Datenmengen, die heutige Automotive-Hardware an ihre Grenzen bringt. Die Frage ist, wie sich ein permanenter Datenaustausch solchen Umfangs Security-seitig effizient begleiten lässt. Selbst mit Maßnahmen zur Steigerung der Leistungsfähigkeit von kryptographischen Operationen, wie der Hardware-Beschleunigung von kryptographischen Algorithmen, lassen sich solche Datenmengen nicht trivialerweise schnell genug verarbeiten. Vielmehr kann durch eine Überarbeitung von Automotive-Hardware-Bausteinen der Overhead, etwa bei der Benutzung der Hardware-Beschleuniger im Hardware-Security-Modul, reduziert werden [2]. Neben der Hardware als solcher, lassen sich Schutzmaßnahmen optimieren, insbesondere durch die Zusammenlegung von Safety und Security zum Beispiel mit kryptographischen Message Authentication Codes (MACs), die auch aus Safety-Sicht qualifiziert sind, Datenintegrität zu liefern [3].

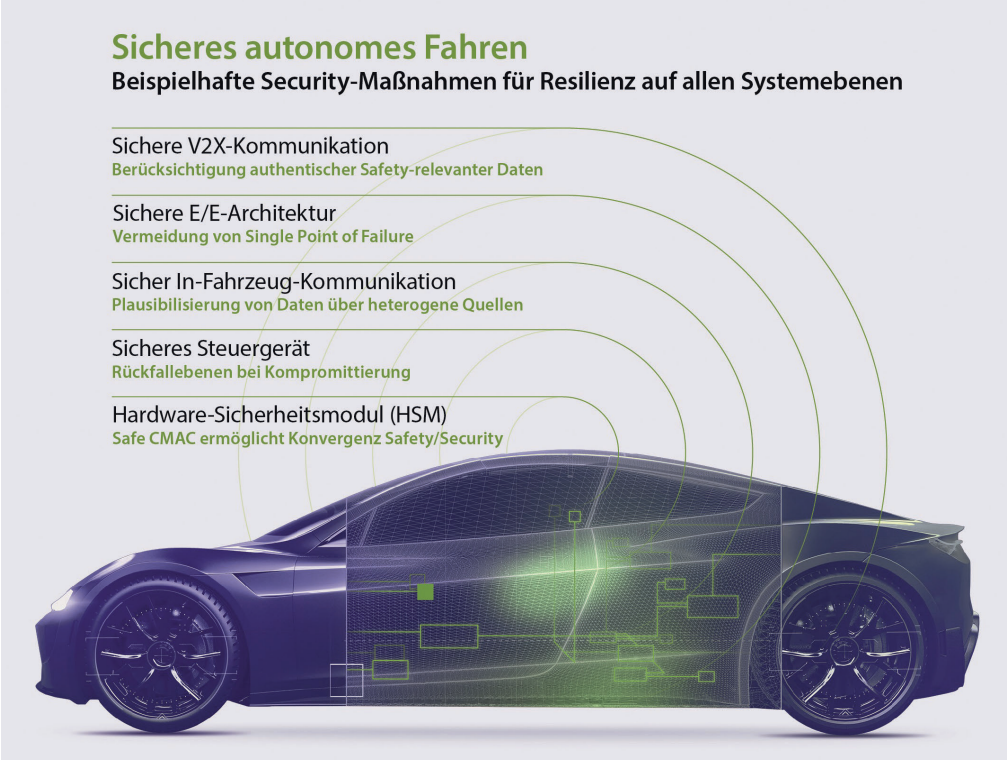

Bild 3: Defense in Depth, die vielschichtige Absicherung mit spezifischen Schutzmechanismen auf allen relevanten Systemebenen, muss die besonderen Implikationen autonomen Fahrens mit einbeziehen. © ETAS

Adversial Attacks

Mit seiner multimodalen Sensorik zur Umgebungserkennung und der Verarbeitung der Sensordaten via künstlicher Intelligenz ermöglicht das autonome Fahrzeug Angriffsparadigmen, die die sensorische Umfelderfassung durch Adversial Attacks gezielt irreführen. Dabei täuschen Angreifer die Wahrnehmung des Fahrzeugs beispielsweise mittels physischer Markierungen oder Aufkleber am Straßenrand. Mögliche Folge: Das autonome Fahrzeug erkennt Objekte, wo keine sind, missinterpretiert Verkehrsschilder oder wird in seiner Bewegungsschätzung beeinträchtigt. Das Fahrzeug kann nicht mehr verlässlich navigieren, und zugleich kann kein Fahrer mehr korrigierend eingreifen. Im Hinblick auf die funktionale Sicherheit wird das Thema im Rahmen der ISO/PAS 21448 „Safety of the intended functionaltity" (SOTIF) behandelt [4]. Für die nötige Robustheit und Verfügbarkeit von autonomen Fahrzeugen müssen künftig mögliche Adversial Attacks auch seitens der Cybersecurity berücksichtigt werden. Dabei sind Schutzmaßnahmen auf unterschiedlichen Ebenen denkbar: im Sensor selbst, bei der direkten Verarbeitung der Sensordaten oder bei deren Fusion.

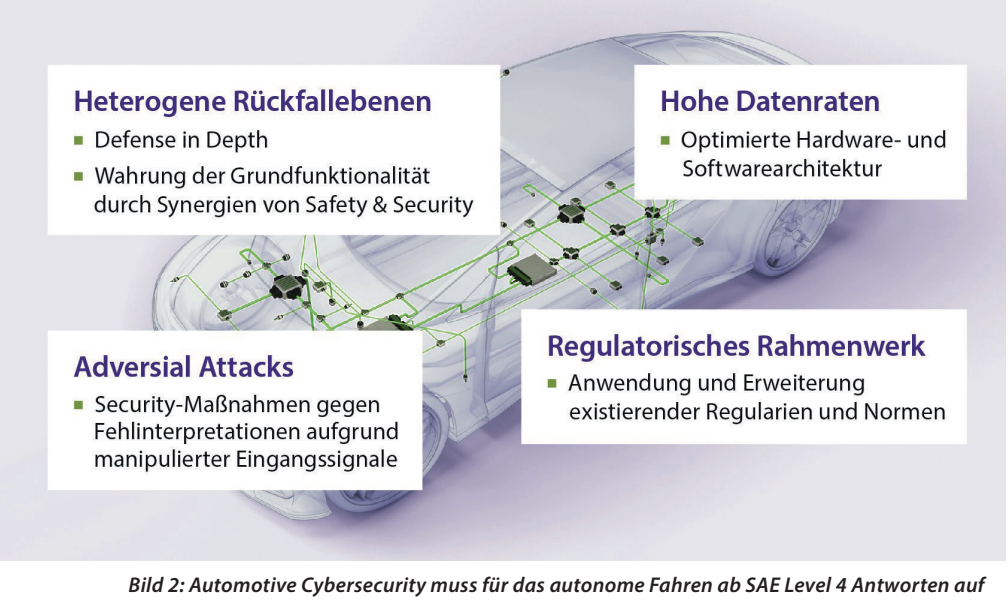

Bild 2: Automotive Cybersecurity muss für das autonome Fahren ab SAE Level 4 Antworten auf spezifische neuartige Herausforderungen finden. © ETAS

Regulatorische Rahmenwerke

Über die letzten Jahre sind regulatorische Rahmenwerke entstanden, die eine risikobasierte, qualitative Bewertung der Angriffsflächen von Fahrzeugen vorsehen, um daraus geeignete Maßnahmen abzuleiten. Mit dem verpflichtenden Nachweis eines Cybersecurity-Management-Systems (CSMS) gemäß UN-R155 auf Organisationsebene und den technischen Leitlinien auf Fahrzeugebene durch die ISO/SAE 21434 ist Security zum integralen Bestandteil der Typgenehmigung geworden [5,6]. Wenngleich diese Regularien sicherstellen, dass Security auf Prozessebene be-

rücksichtigt wird, bieten sie keine spezifischen technischen Lösungen für die Absicherung autonomer Fahrzeuge an. Einen weiteren Ansatzpunkt bildet hier die UN-R157, die die automatische Spurhaltung betrachtet; sie referenziert jedoch im Wesentlichen die UN-R155 bzw. die UN-R156 zum Software-Update-Management. Beachtenswerterweise ist in Deutschland seit Mitte 2021 ein Gesetz zum autonomen Fahren in Kraft. Dieses Gesetz betrachtet Security allerdings nur auf einem sehr hohen Abstraktionsgrad; dazu versteht es sich ausdrücklich als Übergangslösung auf dem Weg hin zu international harmonisierten Vorschriften [7].

Erste grundlegende Schritte hin zu regulatorischen Rahmenwerken fürs autonome Fahren sind also vollzogen. International gültige Regelwerke, die darauf aufbauend einen hinreichenden Schutz vollautomatisierter Fahrzeuge ab SAE Level 4 verbindlich definieren, allerdings stehen noch aus. Es ist jedoch damit zu rechnen, dass Regulierungsbehörden und Standardisierungsorganisationen hier den regulatorischen Rahmen in Inhalt und Umfang weiterentwickeln werden.

Autonomes Fahren: Neue Dimension für Cybersecurity

Zur Verwirklichung des autonomen Fahrens mit Hilfe verteilter Systeme in und außerhalb des Fahrzeugs ist die Orchestrierung von Cybersecurity-Maßnahmen Voraussetzung. Von der ECU über fahrzeuginterne Kommunikation und E/E-Architektur bis hin zu V2X-Kommunikation und vernetzten Diensten liefern sie proaktiven Cyberschutz und sorgen im Angriffsfall für die nötige Resilienz. Etablierte Automotive-Cybersecurity-Mechanismen stellen das Fundament, um den neuartigen Angriffsvektoren und höchsten Safety-Anforderungen zu begegnen. Dabei müssen Security-Maßnahmen im Sinne eines kontinuierlichen Risikomanagements implementiert und über den gesamten Fahrzeuglebenszyklus hinweg alimentiert werden. ■ (eck)

www.etas.com

Quellenverzeichnis

[1] Andy Greenberg: Hackers Remotely Kill a Jeep on the Highway – With Me in It. Unter: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[2] Suraj Ramachandrappa, Raimund Stampa: Hardwarebasierte Cybersicherheit für die nächste Fahrzeuggeneration. ATZelektronik 3–4/2022.

[3] Dirk Bierbaum, Raimund Stampa: Smarte Synthese aus Cybersecurity und Funktionssicherheit, ATZ Elektronik 6/2021

[4] ISO International Organization for Standardization: ISO 21448:2022 Road vehicles – Safety of the intended functionality. Unter: https://www.iso.org/standard/77490.html

[5] UNECE World Forum for Harmonization of Vehicle Regulations: UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Unter: https://unece.org/sites/default/files/2021–03/R155e.pdf

[6] ISO International Organization for Standardization: ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering. Unter: https://www.iso.org/standard/70918.html

[7] BMDV: Gesetz zum autonomen Fahren: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html

Michael Friedrich ist Team Lead Professional Security Services mit Fokus Software-defined Vehicle bei Escrypt, einer Marke von ETAS. © ETAS

Wolfram Gottschlich ist Team Lead Professional Security Services mit Fokus Automotive bei Escrypt, einer Marke von ETAS. © ETAS