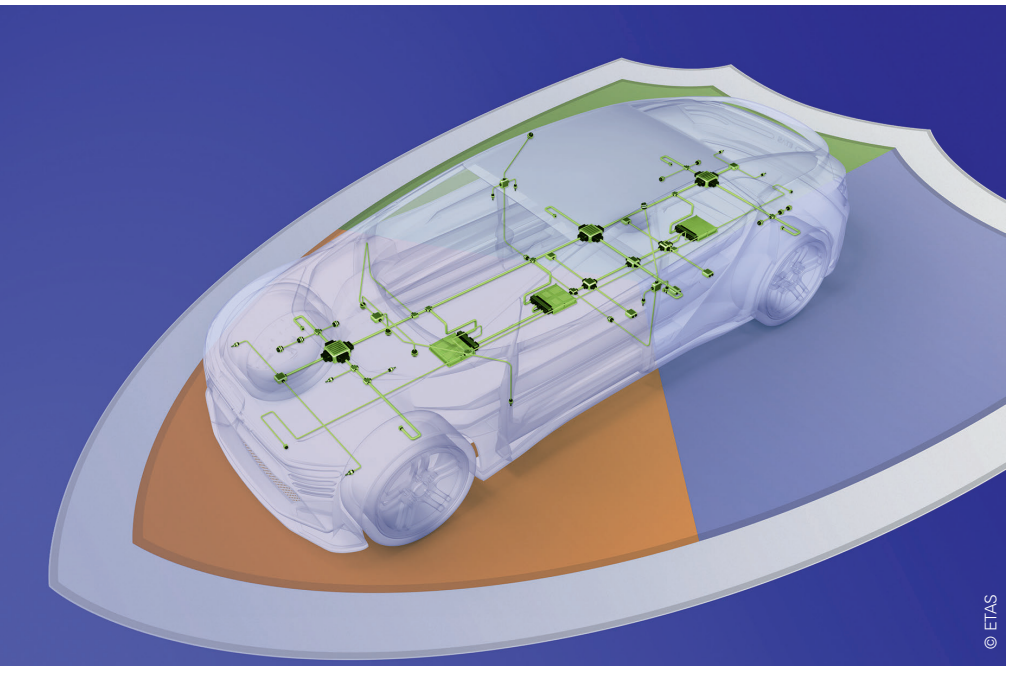
Software-definierte Fahrzeuge

Zonale E/E-Architekturen wirksam absichern

Das Software-definierte Fahrzeug der nahen Zukunft verspricht neue Geschäftsmodelle für Fahrzeughersteller. Geebnet wird der Weg dorthin durch zonale E/E Architekturen. Doch die erhöhte Software-Komplexität und Datenübertragung verlangt nach veränderten Schutzkonzepten gegen Cyberangriffe.

Ramona Jung



Automatisiertes Fahren, Elektromobilität, Over-the-Air-Updates und Flottenmanagement – die Automobilbranche schafft weltweit eine Vielzahl neuer Funktionen und Angebote für ihre Kunden. Einerseits eröffnen sich für die Automobilhersteller damit ganz neue Geschäftsmodelle. Andererseits sind sie gezwungen, diesen Wandel in der Fahrzeugentwicklung in Form veränderter Onboard-Netzwerke technologisch abzubilden. Das Software-definierte Fahrzeug (Software-defined Vehicle, SDV) der nahen Zukunft verlangt nach effizienter, breitbandiger und dynamischer Datenübertragung. Die bevorzugte Lösung: zonale E/E-Architekturen.

Zonale E/E-Architektur für das Software-definierte Fahrzeug

Traditionelle Bordnetz-Architekturen waren funktional eher monolithisch angelegt und durch Steuergeräte definiert; sie waren gekennzeichnet durch überwiegend statische signalbasierte Kommunikation über physikalisch getrennte Bussysteme mit unterschiedlichen Funktionen. Zonale E/E-Architekturen dagegen bedienen sich einer Middleware, die wie eine Art logisches, Software-basiertes Overlay über mehrere Steuergeräte hinweg die Hardware abstrahiert und somit auch erweiterte funktionsübergreifende Kommunikation erleichtert. Ein oder mehrere Vehicle Computer sowie Zonen-Controller steuern und verwalten die Hauptfunktionalität in der zonalen Architektur. Zugleich ermöglicht die Integration neuer Bussysteme, wie etwa Automotive Ethernet oder CAN XL, Echtzeit-Kommunikation mit hoher Bandbreite (**Bild 1**).

Mit einer Architektur, die es gestattet, neue Funktionen unabhängig von Bussystem und Hardware zu implementieren, rufen SDV neue Stakeholder auf den Markt: Neben dem Fahrzeughersteller können nun auch klassische Software-Unternehmen und Mobile-App-Entwickler neue Kundenfunktionen fürs Fahrzeug bereitstellen.

Herausforderungen für die Cybersicherheit

Im Hinblick auf die Cybersicherheit bedeutet dieser Paradigmenwechsel ein Dilemma: Denn Trennung und Isolierung – idealerweise Hardware-basiert – gelten als wichtiges Grundprinzip der Security in fahrzeuginternen Netzwerken. Zonale E/E-Architekturen jedoch durchbrechen die klare Trennung der

© Carl Hanser Verlag, München

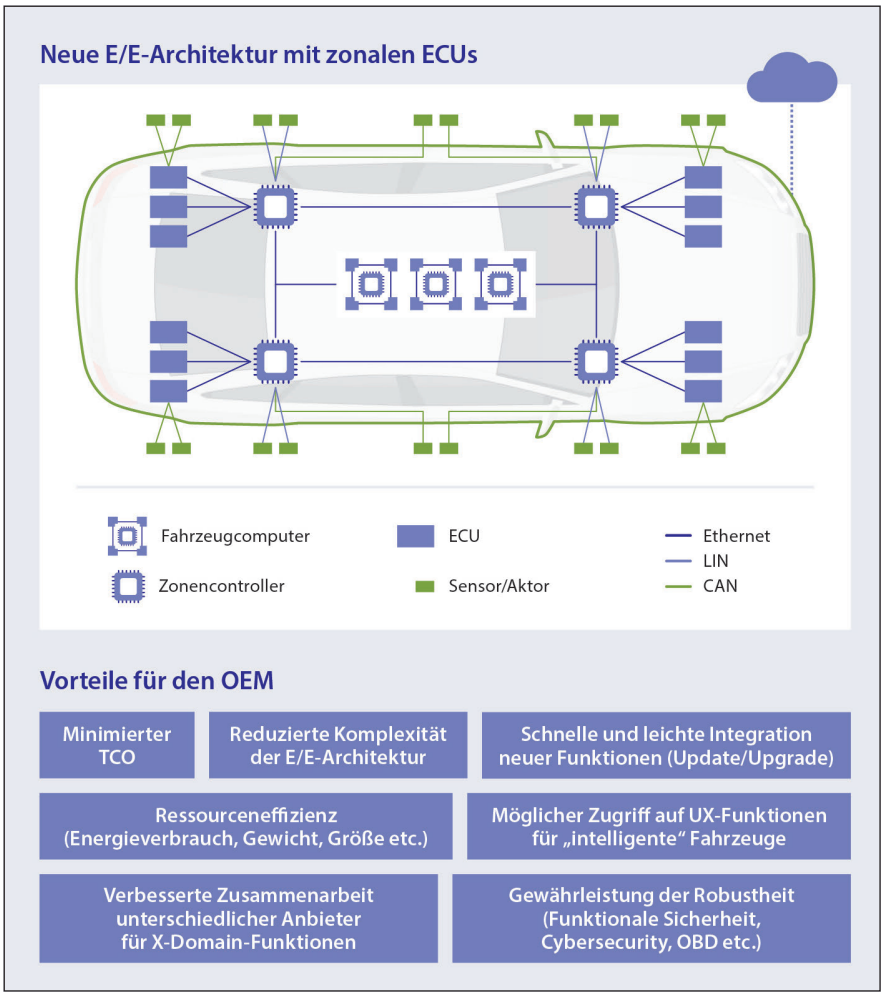


Bild 1: Zonale E/E-Architekturen entkoppeln die Software von der Hardware. Den Fahrzeugherstellern beschert das unmittelbare Vorteile. © ETAS | Bosch

Funktionalität in verschiedenen Domänen; sie verbinden die Endgeräte nicht gemäß ihrer Funktion, sondern nach ihrer Verortung innerhalb des Fahrzeugs. Über dieselben Bussysteme erfolgt die Kommunikation für unterschiedliche Zwecke mit unterschiedlicher Safety- und Security-Relevanz.

Das Trennungs- und Isolierungskonzept kann daher zukünftig nicht mehr der Hardware folgen, sondern muss in Software abgebildet werden. Dabei muss der gesamte Kommunikationsfluss mit einbezogen werden: von der Senderapplikation durch die Software-Architektur und das definierte Netzwerkprotokoll über das spezifische Bussystem zum Empfangssteuergerät, und auch dort wieder durch die Software-Architektur und das Protokoll bis zur Empfängerapplikation.

Hinzu kommt die Software-definierte Realisierung neuer Funktionen wie z. B. automatisiertes Fahren, Anbindung von Cloud Services, Ladetechnik und Fernwartung, die auf der Integration unterschiedlicher branchenagnostischer Service- und Software-Anbieter, wie Google oder Apple, beruhen. Auf Steuergeräten im Auto laufen künftig Webanwendungen von Drittanbietern, die sich auf eine möglichst ständige Anbindung an die Cloud oder andere externe Systeme stützen. Für die Absicherung des Fahrzeugs gegen Cyberangriffe bringt das eine Reihe neuer Probleme:

- Die Webanwendungen selbst als auch die darunterliegenden Betriebssysteme und verwendeten Protokolle sind weit komplexer und vielfältiger als die bisher verwendete Automotive-Software. Das erschwert die Absicherung gegen mögliche Schwachstellen in den Anwendungen.
- Angreifer können die ihnen bekannten Angriffstechniken aus der klassischen IT und mobilen Anwendungen mit wenigen Anpassungen aufs Fahrzeug übertragen.
- Aufgrund der erhöhten Konnektivität von eingebetteten Steuergeräten sind zudem die Gelegenheiten für Angreifer aus der Ferne vergrößert.
- Durch den Mix von funktional unterschiedlichen Komponenten innerhalb der Zonen sowie der übergreifenden Softwarearchitektur können Angreifer direkten Zugriff von außen auf sicherheitsrelevante Fahrzeugfunktionen haben.

Neue Bedrohungen

Dadurch wächst das Risiko, dass Angreifer über bislang nicht bekannte Schwachstellen, sogenannte „Zero-Day-Exploits", Zugriff auf das interne Bordnetz erlangen – und schlimmstenfalls sogar bis zu Safety-relevanten Systemen vordringen. Tatsächlich sind in jüngerer Zeit bereits erfolgreiche Angriffe auf Fahrzeugsysteme über Zero-Day-Exploits in einer Webanwendung demonstriert geworden: In einem Fall erlangten die Angreifer über eine weitere, bereits bekannte Schwachstelle in der veralteten Version des Betriebssystems Kontrolle über das Steuergerät und waren in der Lage, den Kommunikationsfluss über die angeschlossenen Busse auszuspähen. Mit speziell manipulierten Nachrichten gelang es ihnen dann, die Zugriffskontrolle zu umgehen, Brems- und Lenkbefehle zu übernehmen und am Ende das Fahrzeug über eine externe Schnittstelle aus der Ferne zu steuern [1], wie **Bild 2** verdeutlicht.

Gleichzeitig leiten sich auch aus den in zunehmendem Maße gesammelten Daten im Fahrzeug erhöhte Security-Anforderungen ab. Denn Standort-, Bewegungs- oder Sensordaten im Fahrzeug und insbesondere auch personenbezogene Daten, wie etwa Fahrerprofile, wecken Begehrlichkeiten. Nicht nur Angreifern, sondern beispielsweise auch Drittanbietern von Apps im Fahrzeug muss der Zugriff auf vertrauliche Daten verwehrt bleiben. Mit neuen zonalen E/E-Architekturen erhöht sich demnach nicht nur die Zahl der Angriffspunkte, sondern auch die Attraktivität von Angriffen und die damit einhergehenden Manipulationsmöglichkeiten, zum Beispiel auch eine unberechtigte Freischaltung von Funktionen durch Fahrzeugbesitzer.

Sieben Security-Prinzipien für zonale E/E-Architekturen

Die künftigen zonenbasierten E/E Architekturen verlangen daher nach einem neuen ganzheitlichen Security-Konzept,

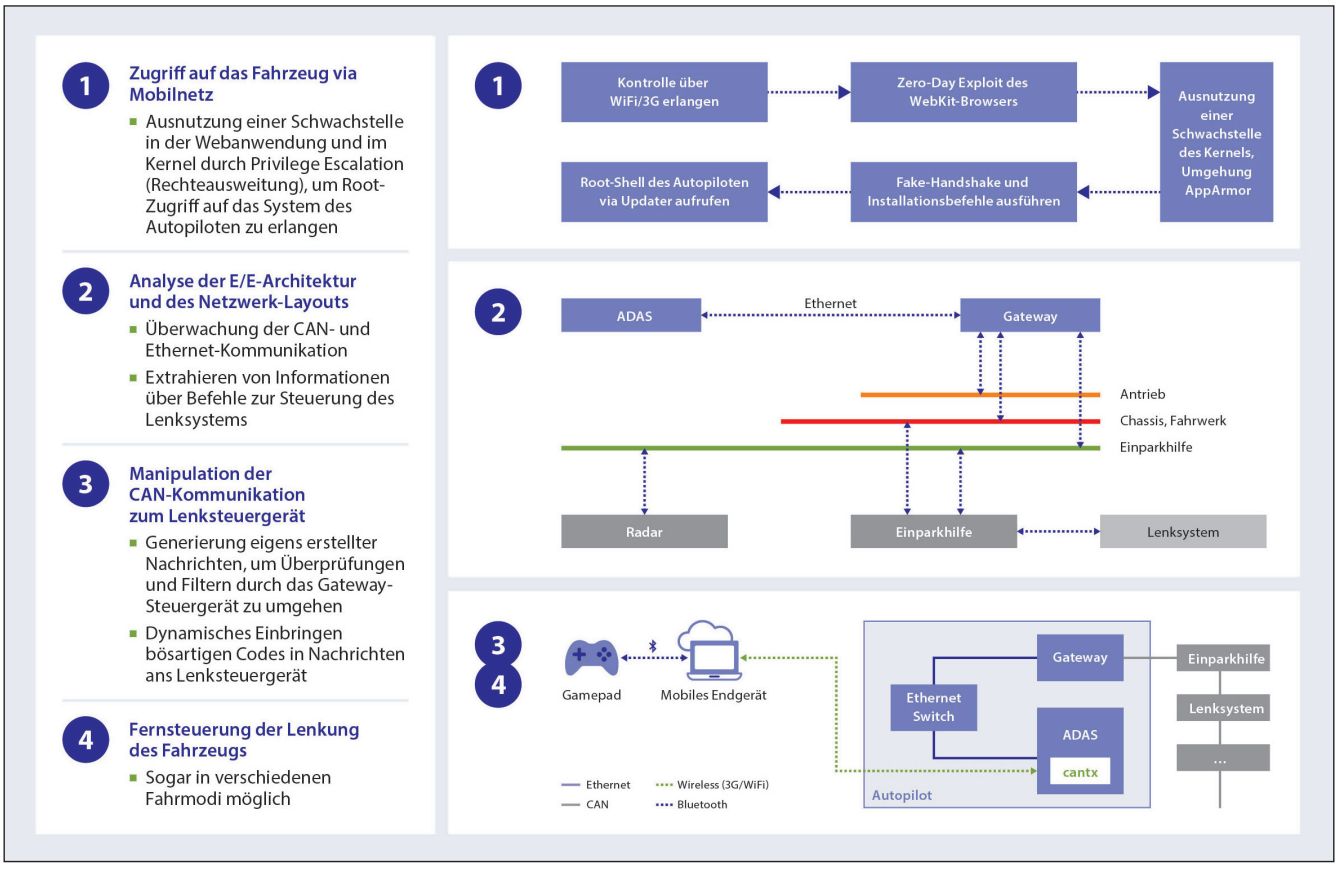


Bild 2: Real ausgeführter experimenteller Angriff auf den Autopiloten eines renommierten Fahrzeugherstellers, ausgehend vom Zero-Day-Exploit in einer Webanwendung © ETAS | Tencent Keen Security Lab

das die schwindende physikalische Trennung der Systeme im Fahrzeug durch konsequente Separierung auf logischer Ebene ersetzt. Ergänzend zu bereits etablierten Security-Maßnahmen im Fahrzeug dienen zur Absicherung der Systeme und Daten dabei Security-Prinzipien (**Bild 3**), die sich in der klassischen IT etabliert haben und auch in E/E-Architekturen Gültigkeit haben:

- Zero Trust
- Least Privilege
- Minimierung der Angriffsoberfläche
- Sichere Kommunikation
- Defence in Depth
- Security by Design
- Kontinuierlicher Schutz

Zero Trust

Das Zero-Trust-Prinzip verbietet, Fahrzeugkomponenten „per se" als vertrauenswürdig anzusehen. Neue oder externe Systeme werden erst nach erfolgter Überprüfung und unter Berücksichtigung möglicher Angriffe von außen oder innen als authentisch und integer, und somit als vertrauenswürdig, eingestuft. Eine Anbindung solcher Systeme ohne vorherige Verifikation ist dann nicht mehr möglich. Stattdessen werden sie beispielsweise innerhalb der E/E-Architektur bei Ethernet-basierten Bussen anhand eines kryptographischen Nachweises über die „Port-basierte Zugriffskontrolle" (Port-based Network Access Control, PNAC) in Switches nach IEEE 802.1X vor Zugriffsberechtigung auf das Netzwerk überprüft.

Least Privilege

Nach dem Least-Privilege-Prinzip dürfen einer Komponente ausschließlich die für ihre Funktionalität zwingend erforderlichen Zugriffsberechtigungen gewährt werden. In zonenbasierten E/E-Architekturen ist hier eine klare Trennung insbesondere dann notwendig, wenn zur Übertragung von Nachrichten zwischen Anwendungen mit unterschiedlicher Funktionalität das gleiche Bussystem genutzt wird, etwa beim Datenaustausch zwischen Vehicle Computer und Zonen-Controller über Ethernet. Auf diese Weise wird zum Beispiel sichergestellt, dass Infotainment-Komponenten keinen oder nur eingeschränkten Zugriff auf Daten haben, die für Safety-Funktionen gesendet werden. Konkret kann das beispielsweise über logische Netzwerksegmentierung mit Virtual Local Area Networks (VLANs) oder Internet-Protocol-Subnetzen (IP) erfolgen.

Wichtig ist: Auch innerhalb eines Steuergerätes muss diese Trennung aufrechterhalten werden, beispielsweise mithilfe eines Hypervisors, der einzelne virtuelle Maschinen voneinander isoliert und unberechtigte Zugriffe zwischen den Systemen verhindert. Und sogar innerhalb eines virtuellen Systems muss ein klares Berechtigungskonzept gemäß Funktion und Security-Relevanz definiert und umgesetzt werden. Eine solche Kontrolle der Zugriffsberechtigungen im Fahrzeug ermöglicht beispielsweise AUTOSAR Adaptive mit dem Identity-and-Access-Management-Modul [2].

Minimierung der Angriffsoberfläche

Fahrzeuge sind in Zukunft über eine Vielzahl von Schnittstellen mit ihrer Umgebung vernetzt, um automatisiertes Fahren oder Elektromobilität zu ermöglichen. Gleichwohl dürfen zukünftige E/E-Architekturen nicht „wahllos" externe Schnittstellen bereitstellen, die dann von Angreifern als Einfallstor verwendet werden könnten. Vielmehr gilt es, externe Schnittstellen wie WiFi und mobile Netze möglichst auf einer Komponente zu koppeln und bereitzustel-

© Carl Hanser Verlag, München

len. Diese muss entsprechend gut geschützt sein und keine weiteren Security-relevanten Funktionen umsetzen. Die klassische IT kennt solch einen Puffer zwischen externem und internem Netzwerk als „Landing Point“ oder „demilitarisierte Zone“.

Sichere Kommunikation

„Secure Communication“ wird in Kombination vorhandener Lösungen wie dem Secure-Onboard-Communication (SecOC)-Modul in AUTOSAR für signalbasierte Kommunikation oder Transport Layer Security (TLS) für Service-orientierte Kommunikation in heutigen E/E-Architekturen schon umgesetzt. In zonalen Architekturen allerdings könnte TLS trotz performanterer Hardware aufgrund der Menge an Services und abzusichernden Daten schnell an seine Grenzen stoßen. Abhilfe versprechen hier Security-Protokolle, die auf physikalischer Ebene arbeiten und eine Absicherung in Echtzeit ermöglichen. Sowohl für signalbasierte Kommunikation über CAN-basierte Busse als auch für Service-orientierte Kommunikation über Ethernet stehen bereits Security-Lösungen in den Startlöchern: Media Access Control Security (MACsec) in AUTOSAR für die Ethernet-Kommunikation auf unterster Ebene (voraussichtlich Ende 2022) sowie der kommende CAN-XL-Standard mit CANsec.

Mittels Firewall- und Filtermechanismen lässt sich heute bereits eine Überlastung des Netzes durch Denial-of-Service-Attacken (DoS) unterbinden. In zonenbasierten E/E Architekturen gilt es, durch hohe Granularität des Schutzes vor DoS-Angriffen nicht nur eine Überlast des Busses, sondern auch eine Überlast bestimmter Nachrichtentypen zu verhindern. So wird sichergestellt, dass selbst einzelne Komponenten jederzeit verfügbar bleiben.

Defence in Depth

Um mehrstufige Angriffe zu unterbinden, bedarf es entsprechender Security-Maßnahmen auf verschiedenen Ebenen. Im Software-definierten Fahrzeug mit zonenbasierter E/E-Architektur muss der Defense-in-Depth-Ansatz jedoch vor allem die verschiedenen Ebenen der Software-Architektur betrachten, die sich zum Beispiel bei der Kommunikation im Ethernet-Protokollstapel zeigen. Erst mit Blick auf die gesamte Übertragungskette von Daten zwischen einzelnen Anwendungen können einzelne Security-Maßnahmen integriert werden. Wichtig hierbei ist eine saubere und sinnvolle Zusammenstellung von Zugriffskontrollsystemen und Berechtigungsmanagement in Form eines ganzheitlichen Konzepts. Das umfasst sowohl die Authentisierung und Autorisierung von Komponenten und Usern als auch die Absicherung und Separierung der Kommunikation.

Praktisches Beispiel für Defence in Depth wäre eine Absicherung der Ethernet-Kommunikation auf physikalischer Ebene durch Zugriffskontrolle mit IEEE 802.1X plus zusätzlicher Absicherung auf logischer Ebene per TLS für bestimmte Daten mit erhöhten Securi-

Wo Schwächen im Code und Angriffsflächen aufgespürt werden müssen, steht secunet bereit. Mit praxiserprobten Testverfahren überprüfen wir herstellerunabhängig vernetzte Fahrzeuge und Komponenten und geben konkrete Empfehlungen für Premiumsicherheit auf der Straße.

secunet.com protecting digital infrastructures

secunet

ty-Anforderungen sowie einer weiteren Kontrolle der Berechtigungen auf Applikationsebene.

Security by Design

Ganzheitliche Cybersecurity verlangt nach einer Integration der Security-Aspekte in den Designprozess der E/E-Architektur. Zwei Punkte sind dabei maßgeblich:

- Security by Default: Grundlegende Security-Maßnahmen sind verpflichtend umzusetzen; Ausnahmen sind nur mit entsprechender Begründung und Genehmigung möglich. Die Security-Maßnahmen gehen dann in die Anforderungen an Kommunikationskanäle und Komponenten ein und finden Berücksichtigung bei der Auswahl der Hardware – beispielsweise durch Integration von Hardware-Security-Modulen in Vehicle Computer oder Zonencontroller, beidseitig authentifiziertes TLS bei externen Ethernet-Schnittstellen oder Absicherung der Kommunikation auf physikalischer Ebene per MACsec bzw. CANsec.
- Krypto-Agilität: Gefahrenlandschaft und Angriffstechnologien entwickeln sich weiter. Dementsprechend muss bereits beim Design der E/E Architektur Luft nach oben eingeplant werden. Für die verwendeten kryptographischen Algorithmen etwa sollten Updates möglich sein, die höhere Schlüssellängen oder sogar die Integration neuer – beispielsweise post-quantum-sicherer – Algorithmen beinhalten. Auch weitere Security-Maßnahmen müssen flexibel und skalierbar gegen zukünftige neue Angriffe aufrüstbar sein.

Kontinuierlicher Schutz

Die größte Gefahr droht zonalen E/E-Architekturen durch die besagten Zero-Day-Angriffe über noch unbekannte Schwachstellen oder neue Angriffsvektoren. Zwar können Security-Prinzipien wie Zero Trust, Least Privilege oder Defence-in-Depth die Auswirkungen solcher Angriffe minimieren. Für den umfassenden Schutz ist es jedoch wichtig, existierende Schwachstellen zu identifizieren und gegebenenfalls sofort zu schließen. Möglich ist das mit einem umfassenden Cybersecurity-Managementsystem (CSMS) gemäß den Anforderungen der UN R155 [3]. Ein Intrusion-Detection-System (IDS) ist dabei ein maßgeblicher Teil, der es ermöglicht, den Security Status im Fahrzeug zu überwachen und Angriffe in der E/E-Architektur zu detektieren – sowohl auf Netzwerk- und Kommunikationsebene als auch auf Komponentenebene.

Fazit: Security fürs Software-definierte Fahrzeug

Zonale E/E-Architekturen liefern dem Software-definierten Fahrzeug der nahen Zukunft die nötige Flexibilität und Performance. Für die Cybersicherheit indes bringen zonenbasierte Fahrzeugarchitekturen neue Herausforderungen mit sich; sie bieten aber auch eine Reihe von Chancen. So können erkannte Schwachstellen zeitnah durch Security-Updates behoben werden und etablierte Security-Maßnahmen der klassischen IT lassen sich für das Fahrzeug angepasst abbilden.

Die dargestellten Security-Prinzipien greifen diese Chancen auf und setzen Leitplanken für eine ganzheitlich sichere zonenbasierte E/E-Architektur. Eine konsequente Implementierung dieser Prinzipien beginnend beim Design der E/E-Architekturen wird zukünftig für die wirksame Absicherung der Systeme gegen unerlaubten Zugriff und den Schutz sensibler Daten im Fahrzeug wichtiger denn je. ■ (eck)

www.escrypt.com

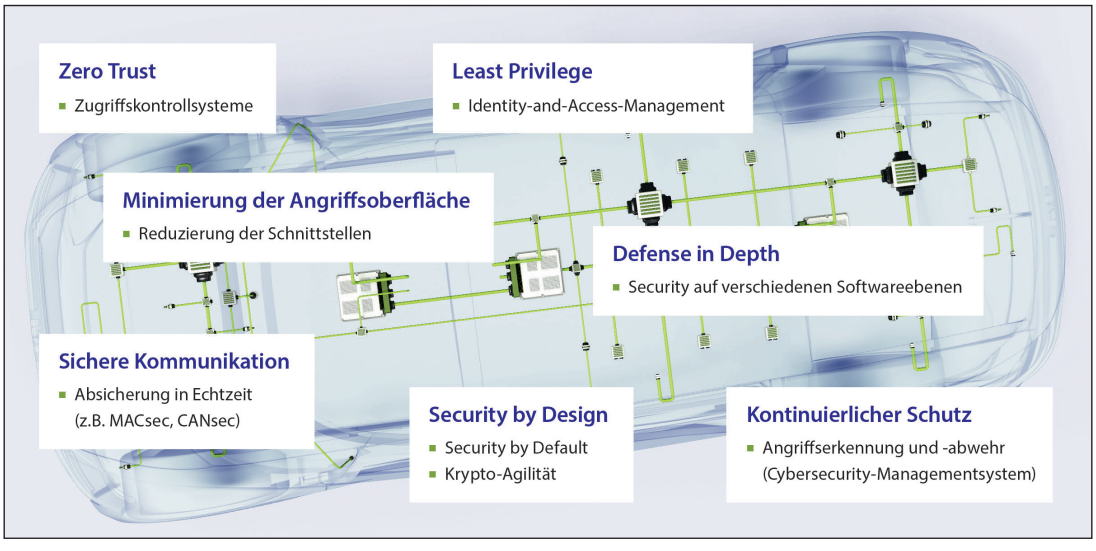


Bild 3: Security-Prinzipien für die Absicherung zonenbasierter Fahrzeugarchitekturen im Überblick © ETAS

Quellenverzeichnis

[1] Tencent Keen Security Lab: Experimental Security Research of Tesla Autopilot. Unter: https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/

[2] AUTOSAR Adaptive Release R21–11. Aktuelle Informationen und Spezifikationen unter: https://www.autosar.org/standards/adaptive-platform/

[3] 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/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

Ramona Jung (M.Sc.) ist Senior Security Project Manager und Expertin für die Absicherung fahrzeuginterner Netzwerke bei Escrypt, einer Marke von ETAS, in Stuttgart. © ETAS

© Carl Hanser Verlag, München