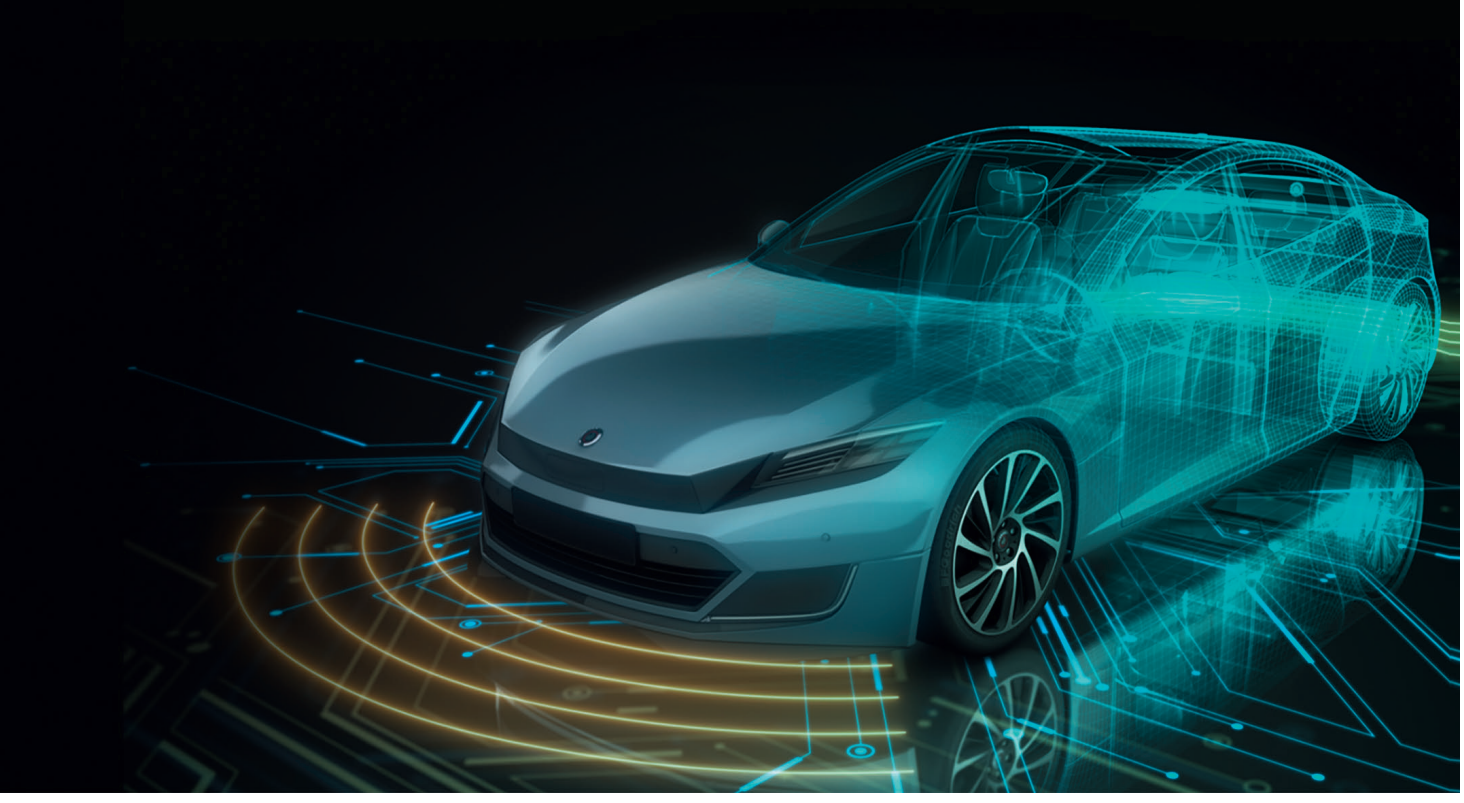

© Siemens

AUSWIRKUNGEN DER MEGATRENDS

Zunehmende **Software-Komplexität** beherrschen

Die Automobilindustrie wird von den Megatrends Automatisierung, Konnektivität, Elektrifizierung und Shared Mobility getrieben. Ein zentrales Thema dabei ist der Umgang mit dem zunehmenden Software-Anteil im modernen Fahrzeug. Denn Sicherheitslücken sind hier keine Seltenheit.

Heutzutage gibt es im vernetzten Auto mehr Codezeilen als in anderen hochentwickelten Maschinen wie dem F-35 Joint Strike Fighter der US Air Force, der Boeing 787 oder dem US Space-Shuttle [1]. Die Hardware ist leistungsfähiger, sodass Millionen Codezeilen durch eine Vielzahl von Systemen ausgeführt werden können, um komplexe Funktionen innerhalb des vernetzten Fahrzeugs zu erfüllen.

Bedrohungen für Cybersicherheit nehmen zu

Zukünftig kommuniziert das Fahrzeug mit seiner Umgebung inklusive anderen Fahrzeugen (Vehicle-to-Everything, V2X). Sicherheit steht dabei an allererster Stelle, daher müssen alle Systeme und Subsysteme sicher sein, während das Fahrzeug in Bewegung ist – oder sich im Leerlauf befindet. Der „Automotive Cybersecurity Report 2020“ (Bild 1) von Upstream Security zeigt eine Versechsfachung über einen Zeitraum von neun Jahren, wobei sich die Zahlen von 2018 auf 2019 verdoppelt haben. Die Grafik zeigt ein Wachstum bei Cyberangriffen von 94 Prozent im Vergleich zum Vorjahr seit 2016. Neue Geschäftsmodelle müssen sich weiterentwickeln, weil Komplexität, Zuverlässigkeit, Risiko und Haftung zu den wichtigsten Faktoren werden.

Zunehmende Cyberangriffe in der Automobilindustrie geben einen neuen Impuls für Sicherheitslösungen und haben zu neuen Vorschriften seitens der Gesetzgeber geführt, um sie weltweit zu verhindern. Das U.S. Security and Privacy in Your Car Act oder das „Spy Car Act of 2017“ beispielsweise definiert Anforderungen an den Schutz vor unbefugtem Datenzugriff und unberechtigten Berichten. Das Gesetz weist die National Highway Traffic Safety Administration (NHSTA) an, Richtlinien für die Cybersicherheit von Fahrzeugen herauszugeben, nach denen in den USA hergestellte Kraftfahrzeuge vor unbefugtem Zugriff auf elektronische Steuerungen und Fahrdaten geschützt werden müssen. 2017 hat das US-Repräsentantenhaus das Gesetz Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act (The Self Drive Act) verabschiedet, das die sichere Entwicklung, Erprobung und den Einsatz von selbstfahrenden Autos sicherstellen soll. China hat ein Komitee für Cybersicherheit in der Automobilindustrie ins Leben gerufen, um den sicheren Betrieb intelligenter, vernetzter und elektrischer Fahrzeuge zu gewährleisten, einschließlich Forschung, Standards, Richtlinien, Ge-

© Carl Hanser Verlag, München

setzen und Vorschriften. Weitere Datenschutzvorschriften beginnen sich herauszukristallisieren, wie die DSGVO der EU, das kanadische Gesetz über den digitalen Datenschutz (PIPEDA) und die Forderung des Verkehrsausschusses des Europäischen Parlaments nach einer EU-Verordnung über den Zugang zu Fahrzeugdaten.

Das Forschungsprogramm für Cybersicherheit im Automobilbereich der NHTSA verfolgt einen Ansatz der Bedrohungsanalyse. Die Bedrohungen werden in sechs verschieden Kategorien eingeteilt:

- Spoofing: Eine Person, ein Programm oder ein Gerät gibt sich als etwas aus, das es nicht ist, indem es Daten manipuliert, um sich einen unrechtmäßigen Vorteil zu verschaffen.
- Manipulation: Vorsätzliche Änderung von Daten zum Schaden des Verbrauchers. Bei vernetzten Fahrzeugen umfasst das Änderungen an Konfigurationsdaten, Software oder Hardware, die in Fahrzeugsteuerungssystemen zum Einsatz kommen.
- Nachweisbarkeit: Der Autor einer Aussage kann die Gültigkeit oder Urheberschaft nicht erfolgreich anfechten.
- Weitergabe von Informationen: Bezug auf diverse Arten von Sabotage im Zusammenhang mit Datenlecks.

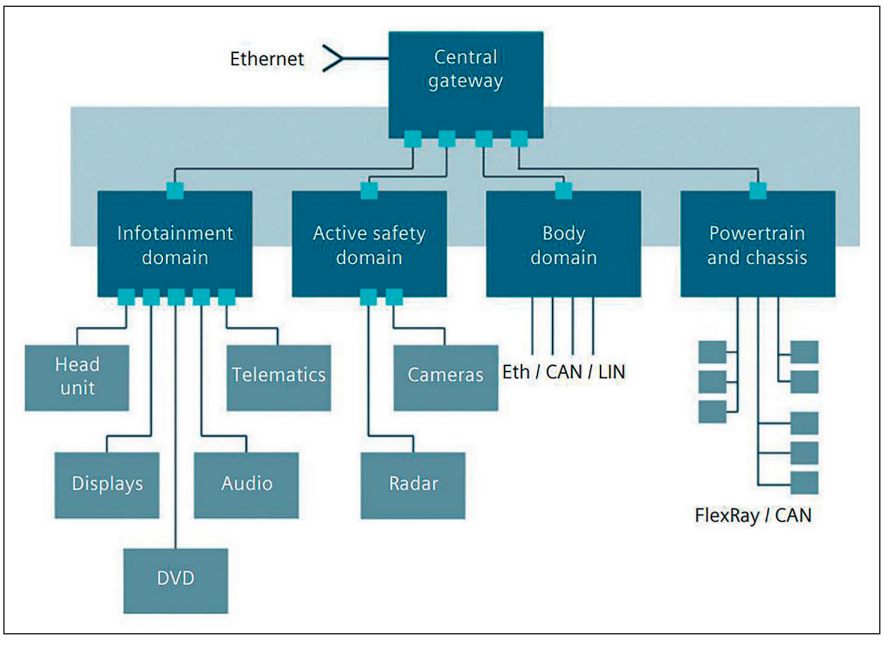

Bild 2: Angriffsflächen und entsprechende Funktionseinheiten. © University of California

- Denial of Service (DoS): Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Dafür kann auch ein Cyberangriff sorgen, bei dem ein Rechner mit übermäßigen Anfragen eines Angreifers überflutet wird, sodass er für legitime Benutzer nicht verfügbar ist, weil seine Systeme überlastet sind.
- Rechteausweitung: Ein Angreifer kann ein Gerät missbrauchen und unbefugte Aktivitäten durchführen, indem er sich unrechtmäßigen Zugriff auf Systemdaten verschafft.

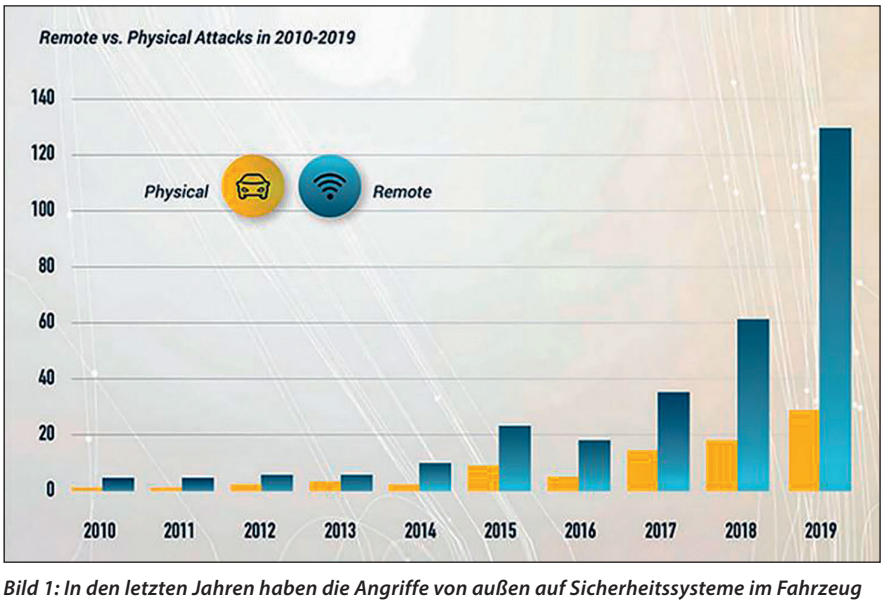

Bild 1: In den letzten Jahren haben die Angriffe von außen auf Sicherheitssysteme im Fahrzeug erheblich zugenommen. Je mehr vernetzte Fahrzeuge auf den Markt kommen, desto stärker steigt das Angriffspotenzial expotenziell. © Upstream Security

Angriffsflächen für vernetzte Fahrzeuge

Durch das Verständnis dieser Bedrohungen können Automobilhersteller vier potenzielle Angriffsflächen an vernetzten Fahrzeugen erkennen:

- Die erste Angriffsfläche ist direkt physisch, einschließlich des Zugangs zum On-Board-Diagnoseanschluss (OBD), zum Ladeanschluss oder zu den Kabelbaumanschlüssen. Ein Auto wird angreifbar, wenn ein Hacker direkten physischen Zugang hat, zum Beispiel beim Händler oder in der Werkstatt für Wartungs- oder Reparaturarbeiten, oder wenn eine zweite Partei Zugang zum Fahrzeug erhalten hat. Das kann etwa ein Parkdienst sein, der einen direkten physischen Angriff ausführen könnte.
- Die zweite Angriffsfläche ist indirekt physisch. Hier wird ein Trägermedium benötigt, um den Angriff auszuführen, wie ein USB-Stick oder eine CD, die die Firmware des Fahrzeugs beschädigt, oder SD-Karten und Firmware-Updates, die alle möglichen Angriffe ermöglichen.
- Die dritte Möglichkeit für Angriffe ist über Funk. Bluetooth und das Mobilfunknetz sind anfällig für drahtlose Angriffe und die zunehmende Vernetzung von Fahrzeugsystemen hat das Angriffspotenzial erheblich vergrößert.

- Die letzte Angriffsfläche ist die Sensortäuschung. Forscher haben gezeigt, dass diese Angriffe in einer Laborumgebung möglich sind. Vernetzte und automatisierte Fahrzeuge setzten häufig LiDAR ein, wodurch Systeme nichts mehr wahrnehmen oder mit falschen Informationen getäuscht werden können, um dem Fahrzeugführer und den Insassen zu schaden. GPS ist eine weitere Technologie mit Sicherheitslücken, die ausgenutzt werden könnten.

Bild 2 zeigt Angriffsflächen, die der Architektur eines Fahrzeugs entsprechen. Dieses grundlegende Schema hebt die Vernetzung innerhalb des Fahrzeugs hervor, einschließlich der Verwendung von Fahrzeug-Gateways und mehreren Fahrzeugbussen, sowie verschiedene Arten von Bereichen: Infotainment, aktive Sicherheit (mit Kameras und Radar) und Karosserie. Elektronische Fahrwerk- und Antriebsstrangsteuergeräte verwenden einen CAN-Bus, der leicht ausgenutzt werden kann. Außerdem werden verschiedene Busse zur Datenübertragung innerhalb des zentralen Gateways angezeigt. Das zentrale Gateway-Steuergerät ist aufgrund seiner direkten Verbindung mit der Außenwelt ein Schwerpunkt für Angriffe.

Es ist ganz klar, dass moderne vernetzte Fahrzeuge mehrere Einstiegspunkte haben, die Hacker als Einfallstor nutzen können. Um jede Art von Cyberangriffen zu verhindern, müssen alle Eintrittspunkte ein angemessenes Sicherheitsniveau aufweisen.

Sicherheit lässt sich in drei Aspekte unterteilen. Der erste Aspekt umfasst Authentifizierung und Zugriffskontrolle. Authentifizierung bedeutet, wer darf in einem Fahrzeug welche Dinge tun. Zutrittskontrolle ist das, was Personen oder Systeme tun dürfen, sobald sie im Fahrzeug sind. Der zweite Aspekt der Sicherheit ist der Schutz vor unberechtigtem Zugriff, Datenlecks oder der Installation schädlicher Software oder Trojaner. Der letzte Aspekt bei der Definition von Sicherheit ist die Erkennung und Meldung von Sicherheitsvorfällen.

Mehrschichtiger Sicherheitsansatz erforderlich

Die Kenntnis der Angriffsflächen innerhalb des vernetzten Automobils bildet die Grundlage für einen mehrschichtigen Sicherheitsansatz. Automobilhersteller müssen die gesamte interne und externe Kommunikation absichern. Eine eingebettete Firewall zum Schutz des Fahrzeugs vor nicht autorisiertem Datenverkehr und Daten oder Signalen, die von einer bösartigen IP-Adresse gesendet werden, muss Teil des Sicherheitspakets sein. Die folgenden Komponenten sind für die Sicherheit eines vernetzten Fahrzeugs von entscheidender Bedeutung:

- Integrierte Firewalls
- Integrierte Firewalls für elektronische Steuergeräte
- Sichere Kommunikation
- Authentifizierung

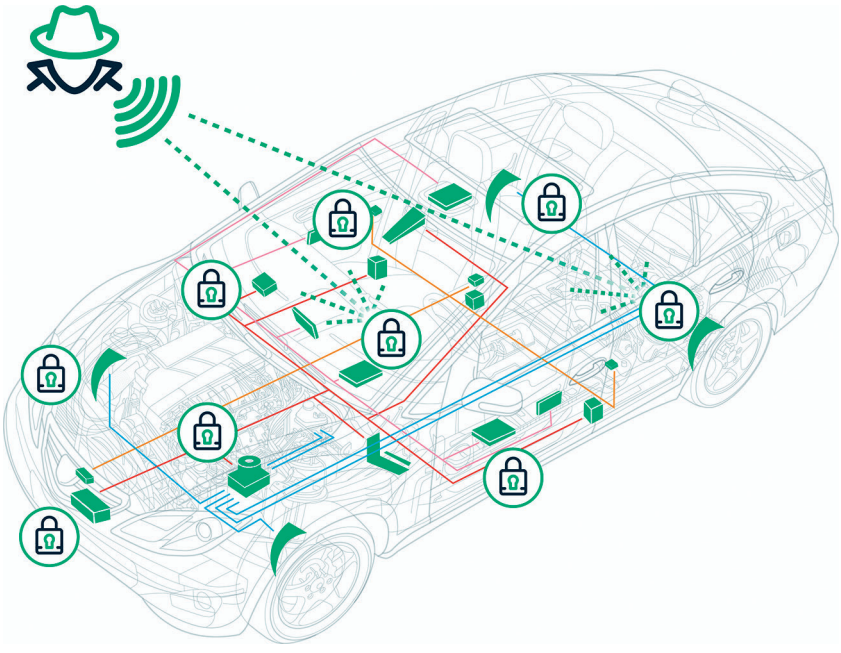

Bild 3: Absicherung von elektronischen Steuergeräten vor Cyberangriffen durch den Einsatz einer eingebetteten Firewall und zertifikatbasierter Authentifizierung. © Sectigo

Integrierte Firewalls

Der Einbau einer Firewall in ein Fahrzeug ist ein hochspezialisierter Prozess, der speziell auf die Umgebung im Automobil zugeschnitten ist. Zum Aufbau der Firewall wird ein Software Development Kit (SDK) direkt in den Kommunikations-Stack integriert, egal ob TCP/IP, CAN oder eine andere vernetzte Lösung. Die eingebettete Firewall muss hochgradig konfigurierbar und flexibel sein, über eine Reihe von elektronischen Fahrzeugsteuergeräten hinweg funktionieren und mit einem Echtzeitbetriebssystem (RTOS) oder sogar in der AUTOSAR-Umgebung arbeiten. Viele Cyberangriffe beginnen damit, dass sie Pakete an das vernetzte Fahrzeug senden und nach Schwachstellen suchen. Wenn die Firewall diese Aktivität also frühzeitig erkennen und sicherstellen kann, dass bestimmte Pakete nicht empfangen oder weitergeleitet werden dürfen, wird ein potenzieller Angriff bereits verhindert, bevor er überhaupt beginnt. Die Kontrolle darüber, welche Ports und Protokolle für den Empfang von Nachrichten für das Fahrzeug verwendet werden, ist entscheidend für den Schutz und die Meldung verdächtiger Aktivitäten.

Integrierte Firewalls für elektronische Steuergeräte

Das Hinzufügen einer Firewall zu einem zentralen Gateway erfordert einen portablen Quellcode, der in das elektronische Steuergerät integriert und konfiguriert werden kann. In die Firewall integrierte Filterregeln blockieren bestimmte IP-Adressen, erkennen unerwünschte Aktivitäten und reagieren schnell, um Angriffe zu verhindern – die Unterstützung verschiedener Arten von Filterfunktionen durch die Firewall (CAN-Bus, regelbasiert, schwellenwertbasiert, statisch) ist entscheidend, einschließlich Stateful Packet Inspection.

Die Protokollierung und Meldung von Angriffen ermöglicht die Intrusion-Detection, also das Erkennen, dass etwas Ungewöhnliches passiert. Das vernetzte Fahrzeug muss in der Lage sein, schädliche Aktivitäten an ein sogenanntes Vehicle-Operations-Center zu mel-

© Carl Hanser Verlag, München

den, damit Sicherheitsteams in der Lage sind, alle erforderlichen Maßnahmen zu ergreifen und diese Informationen an das gesamte Sicherheitsnetzwerk weitergeben können.

Eine Firewall auf einem externen Gateway-Steuergerät verwaltet die Kommunikation mit allen externen Einheiten und dient als Zielscheibe für Angriffe, indem Filterregeln für die gesamte Fahrzeugkommunikation aktiviert werden. Ihre Aufgabe ist es, Angriffe zu erkennen und zu blockieren, bevor sie die elektronischen Zielsteuergeräte erreichen. Eine weitere Option ist eine Firewall auf einem internen Gateway-Steuergerät. Bei mehreren Netzwerken im Fahrzeug ermöglicht ein internes Gateway-Steuergerät die Kommunikation zwischen verschiedenen Netzwerken, um sicherheitskritische Funktionen zu isolieren – die kritischeren internen Systeme sind vor potenziell schädlichem Netzwerkverkehr geschützt. Schließlich lässt sich eine Firewall auf einem Endpunktsteuergerät, dem eigentlichen Steuergerät, das kritische Funktionen im Fahrzeug verwaltet, einrichtet. Zu den Steuergeräten gehören ABS-Systeme, Airbags und Lenkungssteuerung. Es wird daher empfohlen, eine Firewall auf mehreren Endpunktsteuergeräten einzusetzen.

Sichere Kommunikation

Es gibt zahlreiche Anwendungsfälle für sichere Kommunikation, darunter die Kommunikation zwischen dem Fahrzeug und externen Systemen, die V2V-Kommunikation und die Kommunikation innerhalb des Autos. Die V2V-Kommunikation ist heute häufiger und kritischer, daher muss sie geschützt werden. Um eine sichere Kommunikation innerhalb des Fahrzeugs zu erreichen, müssen alle elektronischen Steuergeräte geschützt sein. Wenn eine Kommunikationssitzung beginnt, ist der Ursprung dieser Kommunikation bekannt – daher wird eine Verschlüsselung empfohlen. Die verschlüsselte Kommunikation verwendet IP-Protokolle wie TLS, DTLS und SSH. Läuft die Kommunikation über einen CAN-Bus, kann CANcrypt zum Einsatz kommen. Um Cyberangriffe abzuwehren, müssen alle Daten mit starker Kryptographie verschlüsselt werden.

Authentifizierung

Während einer Kommunikationssitzung (Bild 3) überprüft die Authentifizierung, ob derjenige, mit dem kommuniziert wird, tatsächlich derjenige ist, der er vorgibt zu sein, d. h. ist das andere Gerät oder der andere Prozess wirklich, was es behauptet zu sein? Für die Authentifizierung ist eine Public-Key-Infrastruktur (PKI) zur Verwaltung und Ausstellung digitaler Zertifikate entscheidend. Jedes elektronische Steuergerät muss identifizierbar sein, und PKI-basierte Zertifikate bieten eine starke Authentifizierung für die Kommunikation zwischen Maschinen. Ein weiterer Aspekt der PKI-Sicherheit ist die Code-Signierung, um sicheres Booten und sichere Updates zu ermöglichen. Bei der V2I-Kommunikation ist eine schnelle, automatisierte Ausstellung von Zertifikaten zwingend erforderlich, da das Hosting und die sichere Verwaltung des gesamten Prozesses unerlässlich sind. Wo wird die Zertifizierungsstelle gehostet? Wie erfolgt die Ausstellung von Zertifikaten? Ist sie automatisiert? Ist sie sicher? Wie werden private Schlüssel geschützt?

Schließlich kann ein Automobilhersteller seine eigene interne Strategie zur Absicherung des vernetzten Fahrzeugs mit einem proprietären Sicherheitsökosystem haben. Betrachtet man jedoch die V2I- oder V2V-Kommunikation, bei der Fahrzeuge verschiedener Hersteller auf derselben Straße unterwegs sind, müssen die Fahrzeughersteller ein gemeinsames Ökosystem mit denselben Anforderungen an Sicherheit, Managementfunktionen und andere sicherheitsrelevante Funktionen aufbauen, um die Interoperabilität aller Fahrzeuge auf der Straße zu gewährleisten. ■ (eck)

www.siemens.com

Quellenverzeichnis

[1] Robert N. Charette. This car runs on code, IEEE Spectrum, Februar 2009.

Dr. Ahmed Majeed Khan arbeitet im Senior Engineering Management bei Siemens Digital Industries Software und ist zudem zentraler Ansprechpartner des Unternehmens für das AUTOSAR-Konsortium.

Rechenpower für jede Fahrzeugplattform

Digitalisierung, Vernetzung, autonomes und elektrisches Fahren: Die automobile Zukunft nimmt in den Modellplanungen der Hersteller Gestalt an. Das umfasst Hochleistungsrechner, Software, Sensoren und Aktuatoren der Fahrzeuge sowie Konnektivität für Mobilitätsdienste. Den Kern neuer E/E-Architekturen bilden Hochleistungsrechner, die als Zentralrechner oder Domänen- sowie Zonen-Steuergeräte zum Einsatz kommen können. Hier setzt **ZF** mit der ZF ProAI an, die diverse Anwendungsfeldern für jeden Fahrzeugtyp abdeckt und für alle Stufen des automatisierten oder autonomen Fahrens geeignet ist. Bei einer um 66 Prozent gesteigerten Rechenleistung verbraucht die ZF ProAI dabei bis zu 70 Prozent weniger Strom. Ihre KI-Fähigkeiten sind für Deep Learning optimiert und eine Grundlage für Sicherheitsfunktionen. Der Rechner bietet eine Grafikprozessor-gesteuerte 360°-Fusion aller verfügbaren Sensordaten. Durch seinen modularen Aufbau kann er mit unterschiedlichen SoC-Varianten bestückt werden. Ebenso lässt er sich mit Software des Zulieferers oder von Drittanbietern betreiben. ZF ProAIer bietet eine flexible Rechenleistung von 20 bis 1.000 Tera-OPS. Das sind bis zu eine Billiarde Rechenoperationen pro Sekunde.

www.zf.com

Mit der neuen ZF ProAI präsentiert ZF einen KI-fähigen Hochleistungsrechner, der für alle Stufen des automatisierten Fahrens von Level 2 bis 5 geeignet ist. © ZF Friedrichshafen