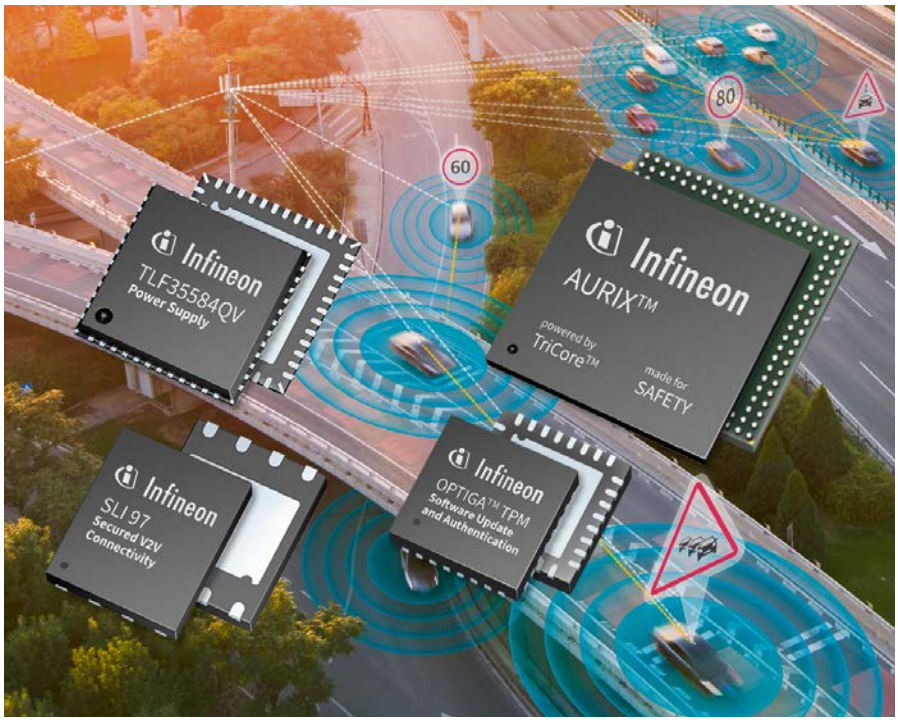
Skalierbare Safety- und Sicherheitskonzepte

Um multidimensionale und offene Connectivity-Systeme im Fahrzeug abzusichern, bedarf es ganzeinheitlicher Safety- und Sicherheitsvorkehrungen für alle Kommunikationsverbindungen – sowohl für die innerhalb des Fahrzeugs als auch für die Kommunikationsverbindungen des Fahrzeugs mit der Außenwelt. Kombiniert man Sicherheits-Know-how aus der Banken- und Sicherheitsbranche mit Fahrzeug-Systemverständnis und Automotive-Safety-Prozessen der Steuergeräte-Entwicklung, lassen sich maßgeschneiderte Halbleiterlösungen für diese Aufgabenstellung erarbeiten, wie das Beispiel eines Software-Updates „over the air" in diesem Artikel zeigt.



© Infineon Technologies

Laut Gesetzgebung soll jeder Neuwagen ab 2018 in Europa mit einem Notruf ausgerüstet sein. Notruf-Informationen werden automatisch an Leitzentralen gesendet, um die Situation abzuklären und gegebenenfalls Hilfe von Rettungsdiensten anzufordern. Noch ist dies ein geschlossenes System.

Die existierende Daten- und Sprachverbindung eignet sich gut, um seitens der Automobilhersteller weitere Dienste anzubieten, wie beispielsweise Ferndiagnose und Werkstatt- und Pannenhilfe. Unterschiedliche breitbandige Kommunikationsschnittstellen dienen als Basis für Software-Update-Funktionen. SOTA (Software Over The Air) hilft Rückrufaktionen der Fahrzeughersteller zu vermeiden sowie erweiterte oder neue Funktionen zu implementieren – auch für Automobile im Feld. Konzepte hierfür sind heute hauptsächlich in Infotainment- und Telematik-Steuergeräten zu finden. Eingeführt werden sie derzeit auch in anderen Steuergeräten wie Motorsteuerung oder Traktionskontrolle im Auto. Nun wird das End-to-End-System durch die Einbindung der Automobilhersteller erweitert. Die SOTA-Funktion ist schon heute als Option bei Premiumherstellern verfügbar.

Zudem öffnet sich das System mehr und mehr solchen Diensten wie Parkplatzsuche, Verkehrsinformationen, ladbaren oder nachladbaren Applikationen (Apps) inklusive Bezahlsystemen und weiteren Internetdiensten. Automobilhersteller werden in der Zukunft Plattformen für multidimensionale digitale Mehrwertdienste anbieten. Weitere Spieler aus der IT- und Kommunikationsbranche mit neuen Geschäftsmodellen und Lösungsansätzen kommen hinzu. Man kann also schon heute von offenen Systemen „Car2Cloud" sprechen, »

die das Auto als aktiven Teilnehmer und Datenknoten im Netz mit vielen anderen Anbietern und Benutzern verbindet (Bild 1).

Sicherheit für Car2Car und Car2Infrastructure

Die weitere Vernetzung von Fahrzeug zu Fahrzeug (Car2Car) und von Fahrzeug zu Infrastruktur (Car2Infrastructure) wird das Autofahren sicherer machen: Unfälle werden vermieden und die Verkehrsleitkontrolle durch Stauerkennung, Priorisierung von Rettungsdiensten und Mautkontrolle unterstützt.

Schnittstellen von persönlichen Geräten wie Smartphones, Tablets oder Speichermedien (wie MP3-Spieler, USB-Sticks etc.) sind in die offenen Gesamtsysteme zu integrieren und z. B. für neue Protokolle flexibel zu halten.

Die jüngste Vergangenheit hat gezeigt, dass solche offenen Systeme Angriffspunkte für Hacker bieten können. Die Angriffe können elektrischer, logischer oder physikalischer Natur sein. Jedoch ist auch bei einem offenen System die unautorisierte Kontrolle über das Fahrzeugnetz zu verhindern. Verhindern muss man außerdem die Manipulationen des Safety-Systems und das unautorisierte Auslesen sensibler Schlüssel. Damit lassen sich die Deaktivierung von Steuergeräten bzw. deren Fehlverhalten vermeiden und der unautorisierte Zugang zu wertvollem Know-how.

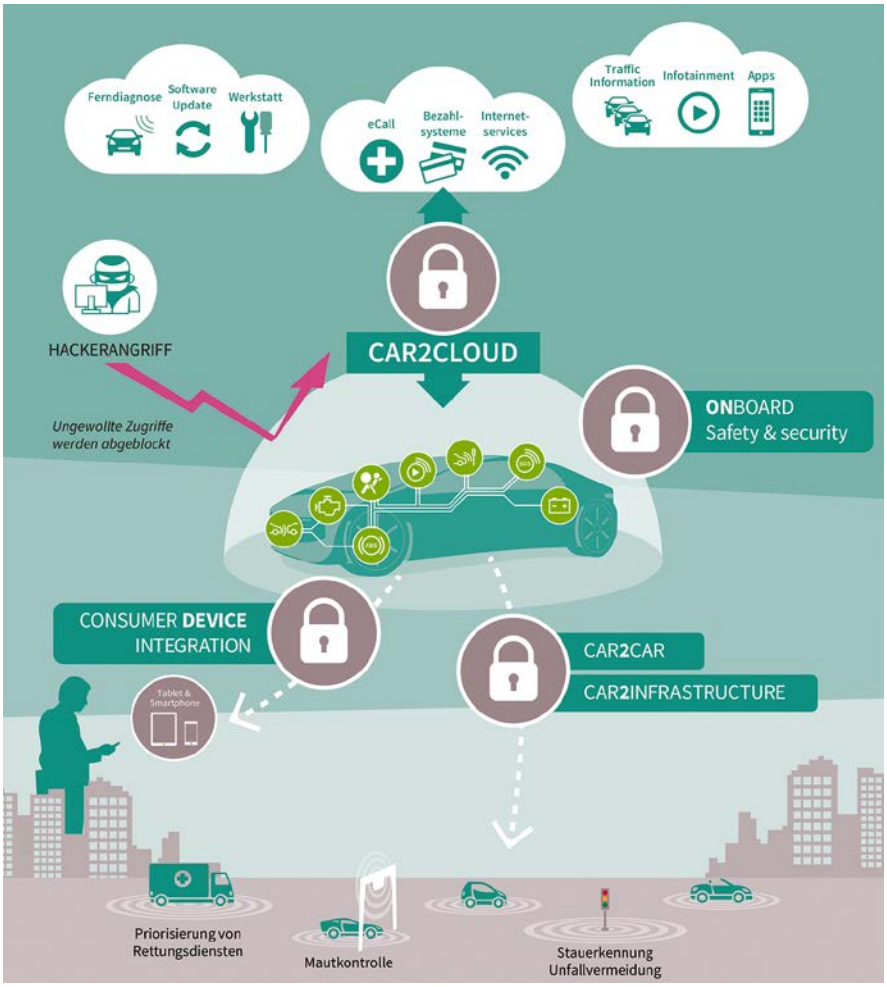


Bild 1: Multidimensionale und offene Konnektivitätssysteme fürs Fahrzeug benötigen Safety- und Sicherheitsvorkehrungen gegen Hackerangriffe. (© Infineon Technologies)

Multidimensionale und offene Connectivity-Systeme

Die Connectivity-Systeme entwickeln sich zu multidimensionalen Funktionslösungen, die durch zusätzliche Mehrwertdienste laufend erweiterbar sind. Zudem steigt die Anzahl der beteiligten Notrufleitzentralen und die der Automobilhersteller. Schließlich werden alle Nutzer des weltweiten Internetnetzes über ihre eindeutig zugeordnete IP-Adresse und Fahrzeugidentifikation einbezogen sein. Zu betrachten sind auch die End-to-End (E2E)-Lösungen; nämlich länderspezifische Einzelanwendungen bis hin zu länder- und branchenübergreifenden Gesamtkonzepten mit den dafür notwendigen Regularien und Vorschriften.

Deshalb ist es unabdingbar, dass eine skalierbare Architektur mit dedizierten Chip-Komponenten zur Verfügung steht und dass diese mit führenden Anbietern von Kommunikations- und Servertechnologien und den entsprechenden Dienstleistungsanbietern abgestimmt ist. Bild 2 zeigt das Zusammenspiel der dedizierten Chip-Komponenten.

Funktionale Sicherheit und Informationssicherheit

Funktionale Sicherheit nach ISO 26262 (Safety) und Informationssicherheit sind Anforderungen für die Steuergeräte der Konnektivitätsanwendungen im Automobil, was mit Spannungsversorgungsbausteinen (z. B. Infineons TLF35584) sowie der 32-bit-Mikrocontroller-Familie AURIX bis hin zu ASIL-D gegeben ist.

Je nach Sicherheitsanforderung des Systemherstellers stehen verschiedene Sicherheitsanker zur Verfügung. Ein solcher Sicherheitsanker kann der integrierte Hardware-Beschleuniger HSM (Hardware Security Module) sein, den jeder Mikrocontroller der Familie AURIX enthält. Die Hardware-Erweiterung HSM ist monolithisch integriert und dient u. a. als sicherer verschlüsselter Speicher mit Krypto-Engine, der ohne Zugangsberechtigung nicht ausgelesen werden kann. Für zuverlässige und sichere Kommunikation im On-board-Fahrzeugnetzwerk bietet Infineon Transceiver für

CAN, CAN FD und Ethernet. Die OPTIGA TPM (Trusted Platform Module)-Bausteine sind dezidierte Sicherheitsmikrocontroller, die sich als hardware-basierte Vertrauensanker im Fahrzeug um den Schutz der geheimen Schlüssel kümmern. Damit ermöglichen sie eine gesicherte externe Kommunikation des Fahrzeuges.

Für die externen Kommunikationsschnittstellen stehen weitere dedizierte Sicherheitsbausteine zur Verfügung. Die Sicherheitscontroller SLI76 und SLI96 werden als embedded SIM (eSIM) für Mobilfunkanwendungen (GSM bis LTE-A) genutzt. Beispiele sind eCall und web-basierte Services. Der SLI97 V2V wurde speziell für den IEEE802.11p WLAN-Standard entwickelt, der als Schnittstelle nach außen sehr wichtig für das autonome Fahren sein wird.

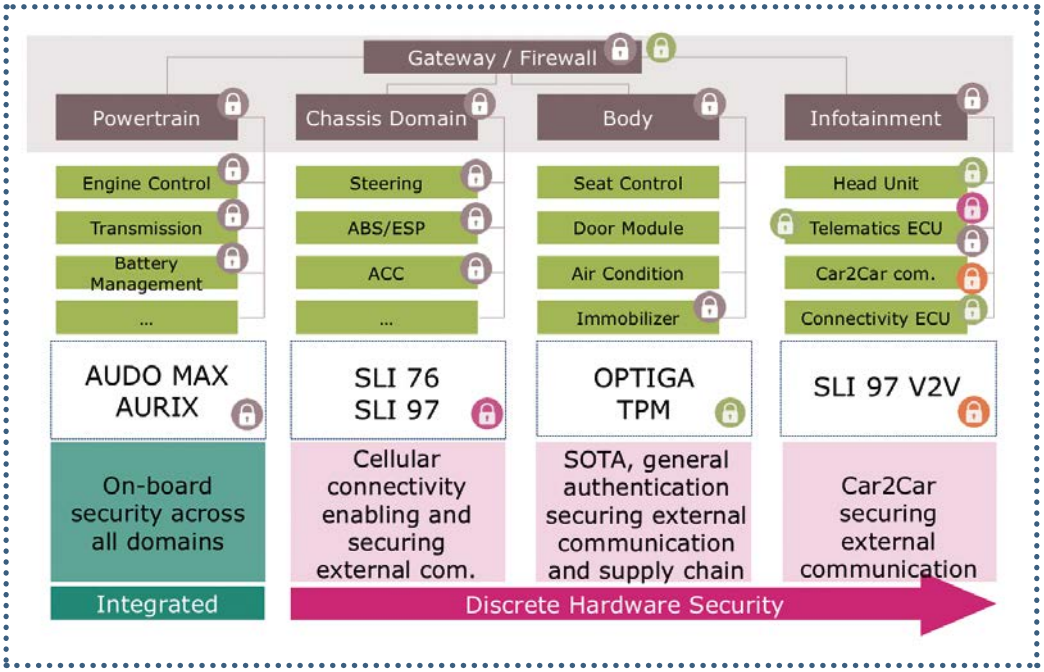


Bild 3: Vereinfachte Board-Architektur mit „Security by Design“. (© Infineon Technologies)

Security by Design

Bild 3 zeigt das Zusammenspiel der gerade beschriebenen Chipkomponenten für offene Connectivity-Systeme. Gezeigt ist eine vereinfachte Board-Architektur im Auto mit den Sub-Domänen Powertrain, Chassis, Body und Infotainment. Nach sorgfältiger Systemrisikoanalyse sind die Sicherheitselemente zu spezifizieren und in die unterschiedlichen Steuergeräte zu implementieren. Dieser ganzeinheitliche Ansatz wird als „Security by Design“ bezeichnet. Grundsätzlich unterscheidet man Schutzmechanismen für das On-board-Netzwerk und für die externe bidirektionale Kommunikation des Fahrzeugs.

Die Nachrichten werden im Fahrzeugnetz hauptsächlich durch Verschlüsselung, Authentifizierung zwischen den Steuergeräten, Zertifikat-Management und Aktivierung von Firewalls zu den unterschiedlichen Sub-Domänen abgesichert. Die skalierbare Mikrocontroller-Familie AURIX mit Sicherheitsbeschleuniger HSM inklusive flexibler Krypto-Software-Bibliothek liefert ein hohes Maß an integrierter Sicherheit, Datendurchsatz und Echtzeitfähigkeit; beispielsweise AES-128 symmetrischer Block Cipher mit bis zu 50 MByte/s für den „Secure Boot“-Modus. Anwendungsfelder sind die Kommunikation zwischen allen Safety-kritischen Steuergeräten wie Radar- und Bremssystemen oder Motorsteuerung und Traktionskontrolle. Und auch für Gateway- und Telematik-Steuergeräte ist AURIX geeignet.

Bei der externen Kommunikation zur Cloud-Infrastruktur oder zu anderen Fahrzeugen muss sichergestellt werden, dass die empfangenen Informationen von einer authentischen Quelle kommen; beispielsweise dem Backend-Server eines Automobilherstellers. Deshalb sind Sicherheitscontroller als Sicherheitsanker notwendig, die alle relevanten Daten und auch die Schlüsselspeicherung gegen Attacken schützen. Sie sind die Sicherheitstür, das „Gate“, zwischen Fahrzeug und Außenwelt.

Für die externe Mobilfunkverbindung bietet Infineon diskrete Sicherheitscontroller der Produktfamilien SLI76 und SLI97 an. Beide werden in »

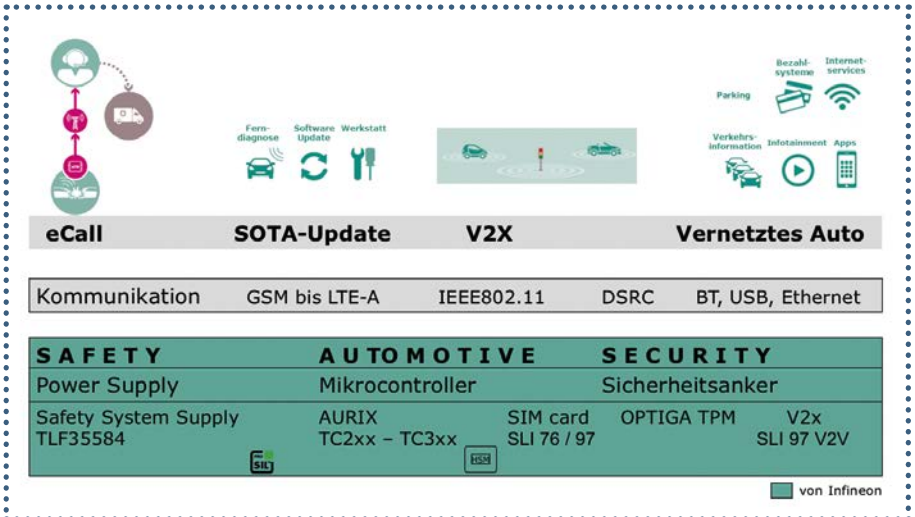


Bild 2: Skalierbares Automotive-Portfolio gepaart mit Security- und Safety-Komponenten für Konnektivität von Infineon. (© Infineon Technologies)

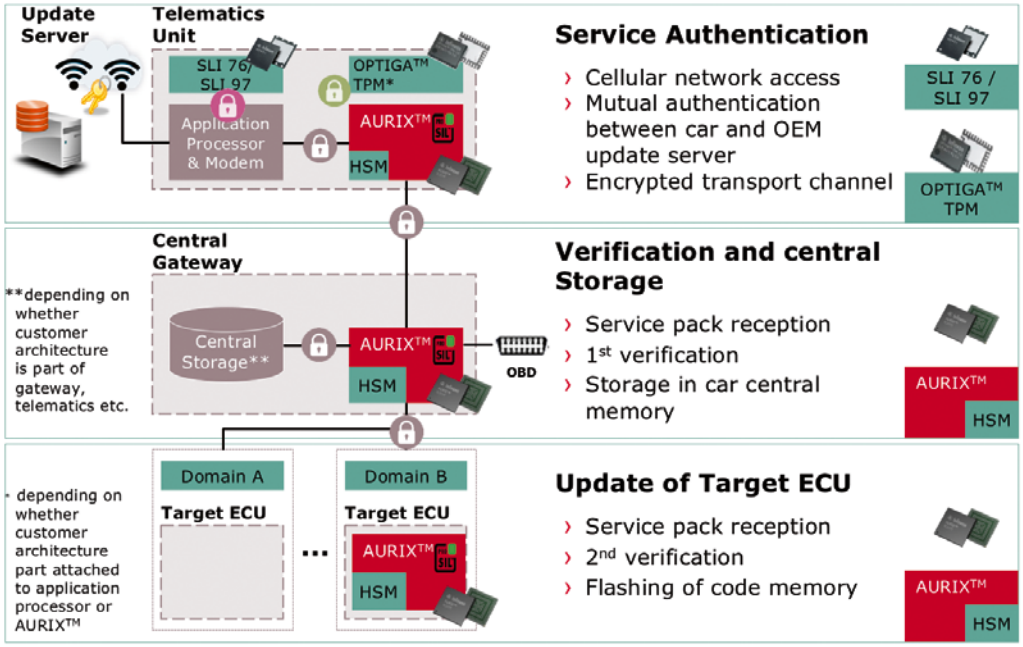


Bild 4: Mehrstufiges Sicherheitskonzept am Beispiel der SOTA (Software Over The Air)-Funktion.
(© Infineon Technologies)

Telematik-Steuergeräten als embedded SIM zur Netzwerkauthentifizierung verwendet.

Die OPTIGA TPM-Sicherheitscontroller eignen sich für zentrale Authentifizierungsaufgaben von externen Quellen. Ihre Stärken bringen sie gerade bei sensiblen Software- und Funktions-Upgrades aus der Ferne sowie beim zentralen Fahrzeug-Schlüsselmanagement ein. Der SLI 97 V2V wurde speziell für die Kommunikation von Fahrzeug zu Fahrzeug und von Fahrzeug zu Infrastruktur entwickelt: Er führt die Authentifikation der eingehenden Nachricht und die Signatur der gesendeten Nachricht durch sowie das Zertifikat-Management und Updates in Echtzeit durch.

Die Sicherheitsbausteine besitzen Common Criteria (CC)-Zertifizierung (ISO 15408). Darüber hinaus sind die geheimen Schlüssel über die gesamte Wertschöpfungskette von Entwicklung über Produktion bis zur Personalisierung in einer sicheren Umgebung eingebracht (Key Injection). Neben der AEC-Q100-Qualifikation sind erweiterte Temperaturbereiche und lange Lebenszyklen gegeben.

SOTA-Partitionierung

Der Lösungsansatz im Bild 4 zeigt exemplarisch ein mehrstufiges Sicherheitskonzept, das für den derzeit bestmöglichen Schutz gegen Angreifer an allen Schnittstellen einer SOTA-Systemarchitektur sorgt. Es sind drei Steuergeräte dargestellt: die Telematik-Einheit TCU, das Gateway und das Zielsteuergerät, das die Software-Updates erhalten soll.

Die Telematik-Einheit erhält zunächst vom Server der Automobilhersteller die Information, dass ein neues Software-Paket für das Auto zur Verfügung steht. Die Freischaltung und Absicherung der Mobilfunkschnittstelle geschieht durch die embedded SIM SLI76/97. Das eingesetzte Sicherheitselement OPTIGA TPM übernimmt die Authentifizierung zwischen dem Auto und dem Server sowie das Erstellen eines verschlüsselten Kanals für die weitere gesicherte Übertragung eines Software-Pakets zur Telematik-Einheit. Nach Erhalt und Quittierung wird die Software an das zentrale Gateway weitergeleitet.

Im Gateway erfolgt die Verifikation des Service-Pakets durch das integrierte Sicherheitsmodul HSM auf dem AURIX, um nachfolgend auf dem zentralen Speicher abgelegt zu werden. Der Speicher beinhaltet die neu abgelegte sowie die momentan aktuelle Softwareversion des Zielsteuergeräts in verschlüsselter Form. Nach einer weiteren Verifikation durch das HSM im AURIX des Zielsteuergeräts erfolgt das eigentliche Aktualisieren der überprüften Software in einem abgesicherten Prozess mit abschließender „Secure Boot"-Funktion im abgestellten Zustand des Autos.

Fazit

Die vielschichtigen Sicherheitsmaßnahmen und Prozesse, die in diesem Beitrag am Beispiel SOTA beschrieben wurden, lassen sich mit zusätzlichen Security- und Safety-Funktionen erweitern. Einerseits kann dadurch die Funktionalität garantiert werden, und andererseits wird das Auto vor Hackerangriffen geschützt, was letztendlich zum sicheren und unfallfreien Fahren auf der Straße beiträgt. ■ (oe)

» **www.infineon.com/aurix**
» **www.infineon.com/car-security**

Dietmar Messner ist System Architect Automotive Connectivity bei Infineon Technologies