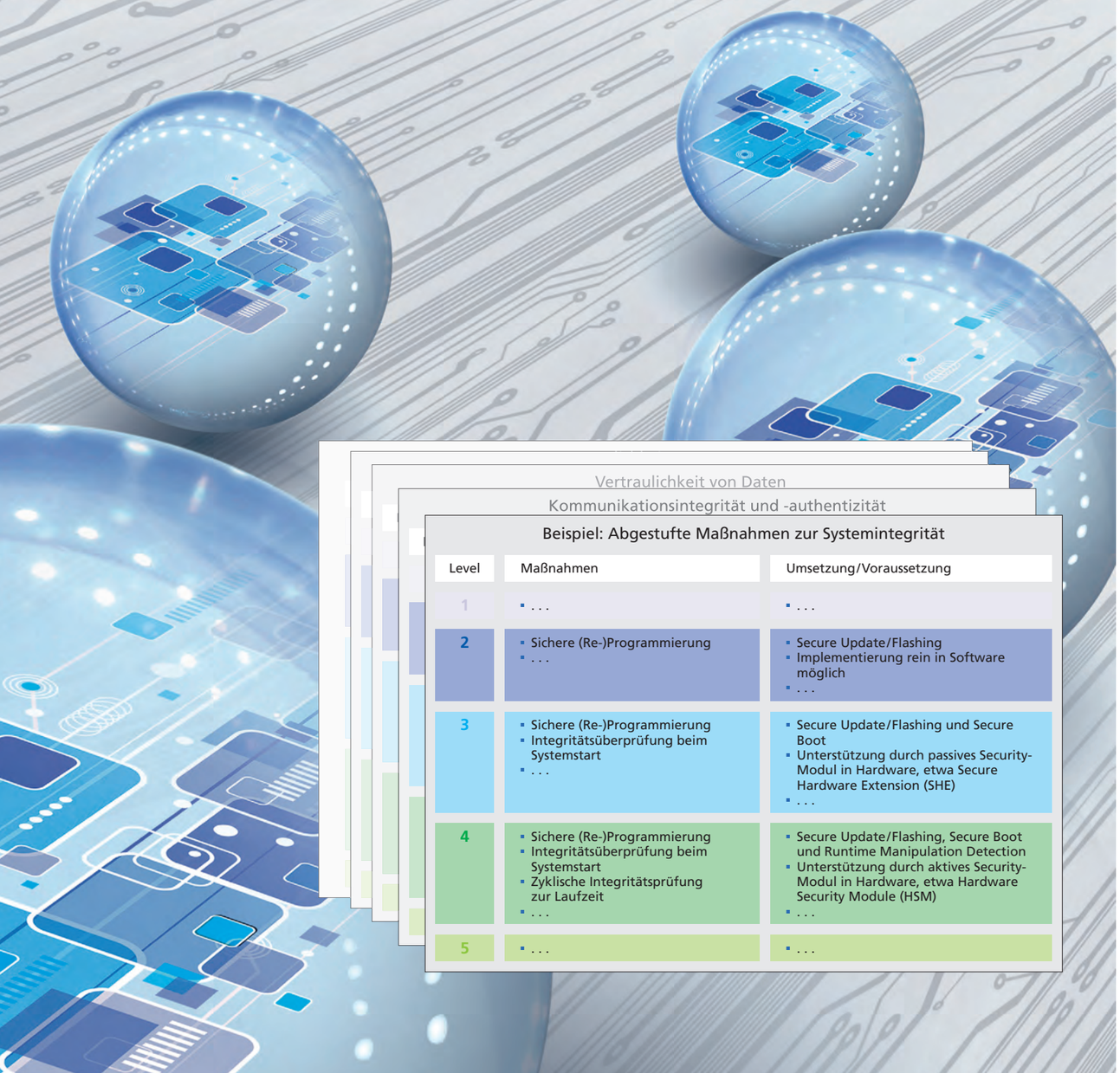
# Safety und Security – ein holistischer Ansatz




Sichere Systeme in der vernetzten Welt erfordern eine umfangreiche Absicherung.

**Vernetzte Fahrzeuge setzen eine neue Risikowahrnehmung voraus**

IT-Systeme im Fahrzeug öffnen sich für die Außenwelt. Das birgt Chancen, aber auch neue Risiken, welche ein grundsätzliches Umdenken in der Risikobewertung und Sicherheitsarchitektur erfordern. Safety und Security müssen künftig stärker ineinandergreifen. Gefragt ist ein holistischer Ansatz, der den gesamten Lebenszyklus und alle Komponenten des Fahrzeugs im Blick hat.

**Eine sonore Stimme** weist auf Sehenswürdigkeiten hin, erläutert historische Orte und streut ab und zu Angebote naher Bars und Shops ein. Die werbefinanzierte Online-Stadtführung im eigenen Pkw basiert auf Vernetzung. Umfeldsensoren leiten ihre Daten an Steuergeräte und die Kommunikationseinheit des Autos, die Kontakt zur Verkehrsleitzentrale und nahen Fahrzeugen hält. Dank des ständigen Datenaustauschs fließt der Verkehr. Unfälle und Staus sind Ausnahmen. Auch der $CO_2$-Ausstoß des Straßenverkehrs sinkt, seit Ampelphasen auf Basis einlaufender Fahrzeugdaten in Echtzeit ans Verkehrsaufkommen angepasst werden. Fahrzeuge auf Parkplatzsuche bringen nichts mehr ins Stocken. Fahrer und Insassen steigen an Haltebuchten aus, ehe webbasierte Systeme ihre Pkws zur nächsten Parklücke leiten. Der Parkassistent kann sein Einparkmanöver anhand von Daten des Pkws vorausberechnen, der bis eben hier parkte.

## Für eine erfolgreiche Vernetzung sind Sicherheitslücken tabu

Diese Vision deutet das Potential des vernetzten Verkehrs nur an. Niemand weiß, welche Geschäftsmodelle die Vernetzung der bisher geschlossenen IT-Systeme von Fahrzeugen ermöglicht. Upgrades von Motorleistung, von Navigations- oder Assistenzsystemen sind im rollenden Internet ebenso denkbar, wie vergünstigte Versicherungstarife auf Basis freiwillig übermittelter Fahrdaten. Allerdings gehen mit der Öffnung für Apps und Upgrades, für Mobilgeräte wechselnder Insassen oder den Car-to-X-Datenverkehr auch neue, zum Zeitpunkt der Entwicklung noch teils unbekannte Risiken einher. Um sie zu beherrschen, ist grundsätzliches Umdenken in der Risikobewertung und Sicherheitsarchitektur erforderlich.

Gefragt ist ein holistischer Ansatz, der den Gesamtlebenszyklus des Fahrzeugs und alle Komponenten in den Blick nimmt und sicherheitsrelevante Funktionen des Fahrzeugs zuverlässig abschirmt. Trotz Öffnung bleibt intrinsische Sicherheit das Ziel. Keinesfalls dürfen Hacker oder über Mobilgeräte eingeschleuste Viren die Sicherheit von Fahrzeug und Insassen beeinträchtigen. Und ohne Zutun des Fahrers muss gewährleistet sein, dass nur autorisierte Anbieter getestete Software aufspielen können. Diese Abschirmung muss in der IT-Architektur angelegt sein.

## Risikoanalyse und -bewertung für den gesamten Lebenszyklus

Damit wird klar: Security als Schutz vor Eingriffen von außen und Safety, welche die Systemfunktionen auch im Notfall gewährleistet, müssen im vernetzten Fahrzeug stärker ineinandergreifen als bisher. Schon vor Beginn der Soft- und Hardware-Entwicklung sollten Security- und Safety-Experten gemeinsam Risiken ermitteln, diese bewerten und daraus abgeleitete Sicherheitsziele formulieren. Hier helfen Bewertungsverfahren, die Wahrscheinlichkeiten und Folgen etwaiger Störfälle analog zur ISO 26262 in ASIL-Level einteilen. Diese grundlegende Analyse folgt dem holistischen Ansatz und sollte fest eingebaute Komponenten ebenso wie Smartphones, Werkstatt-Diagnosegeräte oder Server und Fahrzeuge im Over-the-Air(OTA)-Datenaustausch berücksichtigen, mit denen die Fahrzeug-IT nur zeitweise in Verbindung tritt.

Wenn das Risiko im System erkannt und die Safety- und Security-Anforderungen identifiziert wurden, kann die Software-Architektur erstellt werden. Bereits in diesem Stadium ist zu klären, wie welche Daten in die Steuergeräte gelangen, wer welche Daten lesen und verändern darf und welchen Spezifikationen die späteren Funktionen und Tests folgen. Entscheidend bei zunehmender Konnektivität: Die Fahrzeugsysteme stehen nach der Auslieferung in Interaktion mit der komplexen Außenwelt.

AUTOREN

**Dr. Simon Burton** ist Director Global Embedded Software Services bei der **ETAS GmbH**.

**Dr. Martin Emele** ist Leiter der Product Security Group bei der **ETAS GmbH**.

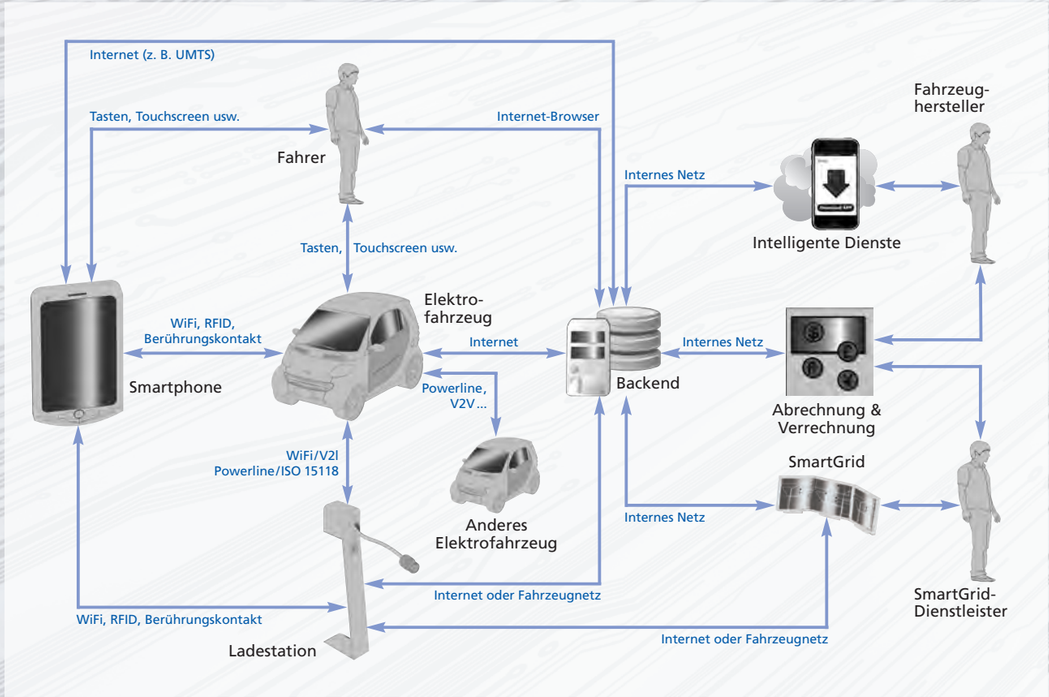
**Dr. Thomas Wollinger** ist Geschäftsführer der **ESCRYPT GmbH**.

Das verändert die Anforderungen an das Risikomanagement und die Sicherheitsarchitektur grundlegend. Zugangsberechtigungen für Fernzugriffe von Werkstätten sind zu klären, Absender eingehender Daten zu überprüfen. Zudem sind kryptographische Daten vor unberechtigtem Zugriff zu schützen; und zwar vom Entwicklungsstart bis zur Verschrottung. Am Ende müssen die individuellen kryptographischen Schlüssel des Fahrzeugs zuverlässig gelöscht werden, um kein sicherheitsrelevantes Know-how in falsche Hände geraten zu lassen.

### Alle Komponenten im Blick behalten

Auch Firmware- und Software-Upgrades Over-the-Air (FOTA/SOTA) oder Apps, die in die Software des Fahrzeugs eingreifen, bergen Risiken. Sie bedrohen aufgrund der verstärkten Interaktion von Steuergeräten, Sensoren und Aktoren den gesamten Verbund. Die Dimension verdeutlichen Versuche, in denen beauftragte Entwickler von außen in Fahrzeugfunktionen eingreifen konnten. So gelang es 2015 einem Team in den USA, an einem fahrenden Testfahrzeug die Bremse zu aktivieren und den Motor abzustellen. Hersteller müssen Vorkehrungen gegen solche Übergriffe treffen, etwa indem sie jedes Fahrzeug durch Firewalls, Gateways und abgesicherte Kommunikation mit individuellen kryptographischen Schlüsseln schützen. Sicheres Schlüsselmanagement wirkt hier dreifach: Wenn jedes Fahrzeug durch individuelle kryptographische Schlüssel geschützt ist, werden Hacker-Attacken erschwert und treffen im Ernstfall nur ein einzelnes Fahrzeug. Obendrein erfüllt der Zwang zur Authentifizierung eine Torwächterfunktion gegen unbekannte Software und ihre Absender.

Die zukünftige Vernetzung der Fahrzeuge bietet zahlreiche Schnittstellen.






### Datenaustausch nur mit authentifizierten Partnern

Professionell aufgesetzte Security-Lösungen mit sicheren Rechenzentren und den entsprechend qualifizierten Mitarbeitern werden künftig über die Teilnahme an der Car-to-X-Kommunikation bestimmen. Daten werden Empfänger nur dann erreichen, wenn Absender vertrauenswürdige Signaturen vorweisen. Hersteller- und branchenübergreifende Key Management-Lösungen helfen den Fahrzeugen zudem, seriöse Informationen aus der Datenflut zu filtern.

Das Etablieren von Security-Lösungen wird also eine Pflichtaufgabe im vernetzten Verkehr. Doch im Ernstfall müssen auch Safety-Lösungen greifen. Systematisches, an Normen wie der ISO 26262 orientiertes Engineering stellt sicher, dass auch bei Angriffen oder fahrlässiger Virenkontamination alle wichtigen Fahrzeugfunktionen aufrechterhalten bleiben.

Dafür ist es wichtig, sicherheitsrelevante Bereiche zuverlässig gegen den Einfluss nachträglich installierter Software abzuschirmen. Dazu dienen Lösungen wie der ETAS Hypervisor RTA-HVR, welcher ein Steuergerät in mehrere strikt voneinander getrennte virtuelle Steuergeräte partitioniert. Ihre Funktionen sind damit komplett von Außeneinflüssen abgeschirmt. Es gilt, vorab abgeschirmte Kernbereiche zu definieren; angesichts reger Interaktion der Steuergeräte im Fahrzeug setzt das viel Erfahrung sowie eine bewährte Methodik und effiziente Werkzeuge voraus. Seien es Möglichkeiten, Soft- und Hardware in-the-Loop zu testen, Protokolle aus dem Bereich funktionale Sicherheit oder ein Instrumentarium zur Echtzeit-Überwachung von Speicherzugriffen, Rechenzeiten und Übertragungsraten. Nicht zuletzt gehören Mitarbeiter dazu, die sich in dieser Entwicklungsumgebung sicher bewegen und mit Normen und Branchenstandards wie z. B. AUTOSAR vertraut sind.

### Vorhandenes Know-how nutzen

All das finden Kunden bei ETAS. Das modulare Angebot beginnt mit Know-how und langjähriger Erfahrung in der Planung, Umsetzung und Prüfung von sicherer Embedded Software, geht mit AUTOSAR-konformen Betriebssystemen sowie mit Protokollen zur sicheren Kommunikation weiter und endet nicht mit Werkzeugen wie dem Hardware Security Module (HSM) oder besagtem Hypervisor RTA-HVR. Letzterer wird Automobilherstellern künftig erlauben, ausgewählte Bereiche von Steuergeräten für eigene Updates und Upgrades zu reservieren. Auch das ist ein Stück Sicherheit im Zukunftsmarkt der Konnektivität. Darüber hinaus stehen modulare Security-Lösungen der ETAS-Tochtergesellschaft bereit: Sie reichen von der Lizenz für Kryptographie-Software bis zum kompletten Key Management über den Lebenszyklus aller verkauften Fahrzeuge hinweg; inklusive der Abwicklung in Hochsicherheitsrechenzentren.

### Mit Know-how zu bezahlbarer Risikominimierung

Schon aus Kostengründen wird es im vernetzten Fahrzeug unmöglich sein, jedes Steuergerät komplett abzuschotten. Kompromisse sind notwendig, die allein auf Basis von Risikoanalyse und -bewertung gefunden werden können. Dafür ist der Gesamtblick auf das Sicherheitskonzept aller Fahrzeugsysteme unabdingbar. Ist eine Funktion aus Security-Sicht besonders bedroht, lassen sich für den Ernstfall Routinen bis hin zur koordinierten Abschaltung implementieren. Systematisches Ineinandergreifen von Security- und Safety-Ansätzen ist wichtig, weil künftige Bedrohungen nicht bekannt sind.

Um vernetzte Fahrzeuge gegen unbekannte Risiken zu wappnen, hilft nur die Verbindung aus adäquatem Key Management und sicherer Auslegung der Fahrzeugsysteme. Die Idee, erst bei konkreter Bedrohung zu reagieren, greift zu kurz. Grundlegende Mängel einer Sicherheitsarchitektur sind per Update nicht behebbar. Ohnehin sollten lästige Sicherheits-Updates wegen der begrenzten Datenübertragungsraten so selten wie möglich erfolgen.

### Fazit: Risikowahrnehmung anpassen – Maßnahmenpakete schnüren

Die Vernetzung der Fahrzeuge setzt eine neue Risikowahrnehmung voraus. Die Masse von Fahrzeugen, die Frequenz ihrer Nutzung und ihre Anbindung an den externen Datenverkehr erhöhen die Wahrscheinlichkeit von Störfällen. Um daraus potentiell resultierende Schäden zu minimieren, müssen bislang oft isolierte Safety- und Security-Lösungen stärker ineinandergreifen.

Eine holistische Gesamtbetrachtung der Risiken im Vorfeld der Entwicklung ist die Grundvoraussetzung, um vernetzte Fahrzeuge zuverlässig gegen heutige und zukünftige Risiken abzusichern. Dabei muss über den gesamten Lebenszyklus hinweg die Maxime „Safe and Secure by Design“ gelten.