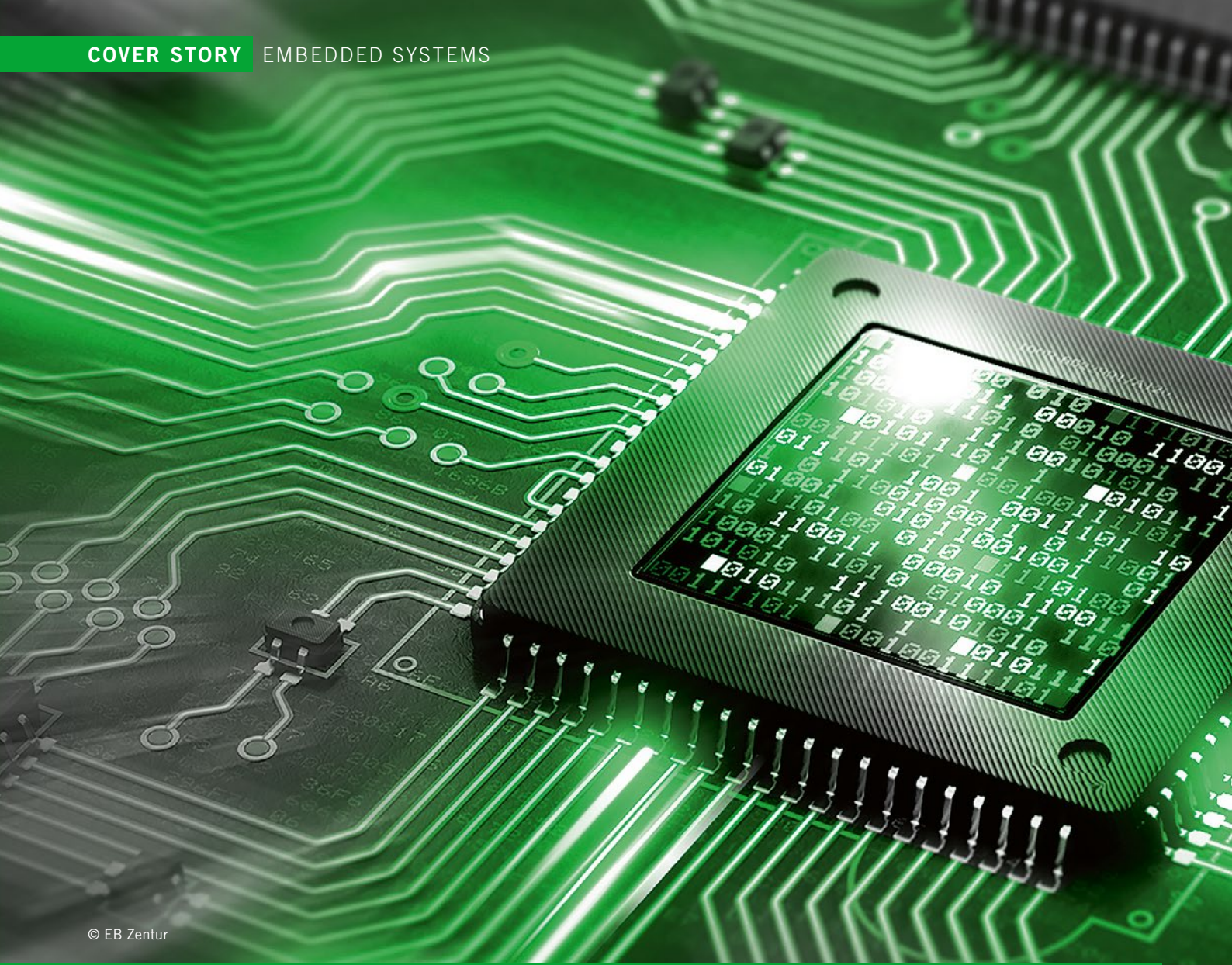
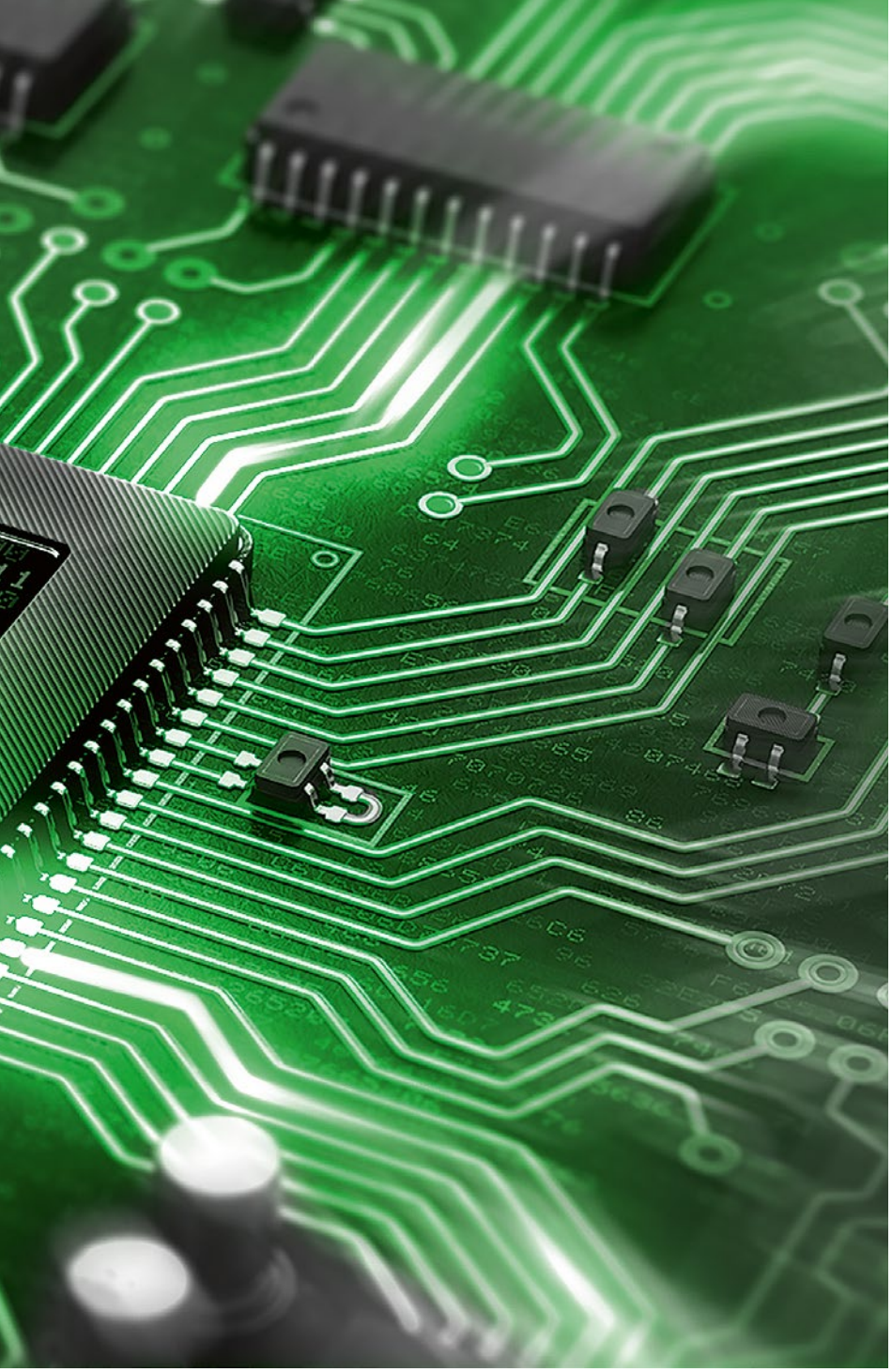




# Security for Connected Vehicles throughout the Entire Life Cycle

Over-the-air software updates are special requirements for the security architecture inside and outside the vehicle. However, they are also essential to keeping a vehicle safe and secure throughout its life cycle. For connected vehicles, automotive supplier Continental uses a holistic connectivity approach – from the vehicle architecture and human-machine interaction to the backend. The subsidiary company Elektrobit offers – in collaboration with Argus Cyber Security – end-to-end security solutions and wireless update solutions for all connected electronic components.



AUTHOR

**Martin Boehner**
is Head of Product Management Security & OTA at Elektrobit in Erlangen (Germany).

## CHALLENGES

The consulting firm Roland Berger expects manufacturers to sell more than 60 million connected vehicles annually worldwide by 2021. Already today, telematics systems in modern vehicles are always online. Increasing connectivity enables additional functions not only when upgrading models, but also over a vehicle's entire life cycle. In addition, the option to regularly install updates and adaptations must be available during the entire life of the vehicle. This is the only way to ensure the vehicle's safety and security.

## CONNECTIVITY INCREASES VULNERABILITY

Providing new software Over the Air (OTA) is a fast and easy way to update vehicle software. At the same time, however, this method increases the number of potential entry points for cyber security attacks. Communication channels such as a regular connection to the backend, Car2X, Wi-Fi, Bluetooth, remote control via apps, OBD II, radio transmitter keys, and so on essentially represent potential gateways for hacker attacks. Aside from the obvious risks such as data loss or malfunctions, these scenarios pose additional risks to car manufacturers, which include damage to their reputation with customers and business partners, cost risks for recalls or countermeasures, and customer dissatisfaction, all the way through to liability risks and potential legal consequences.

On the other hand, connectivity functions allow manufacturers to monitor the vehicles' state and install security updates when necessary. This makes security and connectivity interdependent.

The security philosophy of Elektrobit (EB) is based on three critical pillars, **FIGURE 1**: Car makers should always be able to prevent, understand, and respond to cyber threats. A proactive and comprehensive approach is therefore required to provide end-to-end solutions at all levels. This means that access to the vehicle's hardware is protected such that it can only take place when authorized: Each single Electronic Control Unit (ECU) may only be accessed with authorization using a unique hardware key. Accordingly, the security measures must be embedded in the vehicle architecture: Inside and outside the vehicle, all interfaces and network functions must be systematically protected against unauthorized access and manipulation. In addition, the data flow must be permanently monitored and checked for integrity in order to identify tampering of any kind.

This starts with the individual ECU whose vehicle hardware is protected

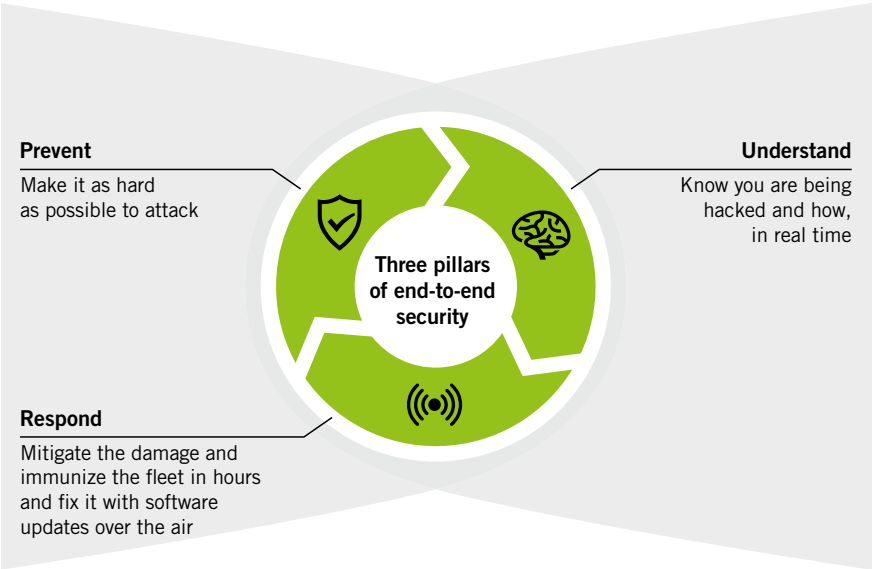



**FIGURE 1** The three pillars of permanent vehicle security at Elektrobit (© Elektrobit)

such that only authorized changes can be made. Ultimately, the entire vehicle architecture is required to consider security aspects in order to have the smallest attack surface possible.

## CHALLENGES FOR SECURITY IN THE CONNECTED VEHICLE

With connected and autonomous driving, security is becoming increasingly important to development and design. Cyber attacks essentially threaten each connected element in the entire chain – from the individual ECU and the overall vehicle to the systems in the backend. In the vehicle, this threat not only affects the communication interfaces of the telematics and infotainment systems but potentially all ECUs. This has particularly serious consequences for safety-related components such as steering and braking systems. However, attack scenarios change as connectivity grows: While ECUs and other electronic components of a non-connected vehicle can be attacked via Bluetooth, remote access, OBD, or USB interfaces only in the direct vicinity, various wireless connections make the connected vehicle vulnerable to attacks from all over the world. Depending on the scenario, the attack affects not only a single vehicle but in an extreme case the entire fleet.

Fast and up-to-date, state-of-the-art protection through OTA software updates is essential to connected driving. A modern vehicle is controlled by 70 to 100 ECUs whose software is based on up to 100 million lines of code. One can only guess how complex this software is: The control software for the particle accelerator built by CERN and Facebook's software apparently have only half the number of code lines. As vehicles increasingly connect to external services, the significance of software will grow even more over the coming years. The life cycles of software are significantly shorter than the life cycles of automotive hardware. In addition, cyber security threats change continuously over a vehicle's life cycle.

The threat scenarios range from manipulating speedometers and spying on vehicle occupants to compromising safety functions up to and including unauthorized remote control of vehicles. Argus Cyber Security, an Israeli subsidiary of EB, specializes in automotive cyber security. Experts from Argus have already revealed a number of potential vulnerabilities in connected vehicles: For example, Argus was able to stop the engine of a moving vehicle using a remote diagnostics dongle. Via Bluetooth, the team of experts managed to bypass security mechanisms and inject messages into the internal vehicle network. The team additionally discovered multiple vulnerabilities in connected ECUs. This allowed Argus to take control of a truck fleet and stop it while in motion using SMS text messages. The insights provided by this penetration testing are directly incorporated into products and solutions.

## PROTECTING CONNECTED VEHICLES

Given the complexity of the overall systems and the high degree of connectivity, a comprehensive security architecture is essential. This architecture must consider all elements and place appropriate security measures at the right locations in the system. On the one hand, this ensures that not every element is required to become its own "maximum security island." On the other hand, due to multiple fallback levels, safe operation can be maintained, if necessary, with restricted functionality, and remedial action can be taken.

The security architecture takes account of the vehicle components and their connections and interfaces as well as the backend and, if applicable, any connected end devices. The concept therefore covers all the layers affected inside and outside the vehicle environment: individual components and ECUs, bus systems inside the vehicle, external interfaces and protocols (including WLAN, for example) as well as end-to-end encryption and protection of all relevant services. This not only ensures system integrity and prevents attempted misuse, but also meets the ever-increasing legal requirements for data privacy and information security.

To achieve these goals, Elektrobit offers solutions at different levels. For example, an EB zentur HSM implementation, **FIGURE 2**, is used to ensure, in a single ECU, that cryptographic key material is securely stored and securely used with hardware-accelerated cryptography. In addition, secure boot can be used to constantly ensure the integrity and protection of an ECU's start process.

Depending on the ECU, the cryptographic options in hardware and software for other functions are provided via the security stack according to Autosar Classic (EB tresos) or Autosar Adaptive (EB corbos), **FIGURE 3**. In this context, basic applications are to authorize operations such as updates or configuration

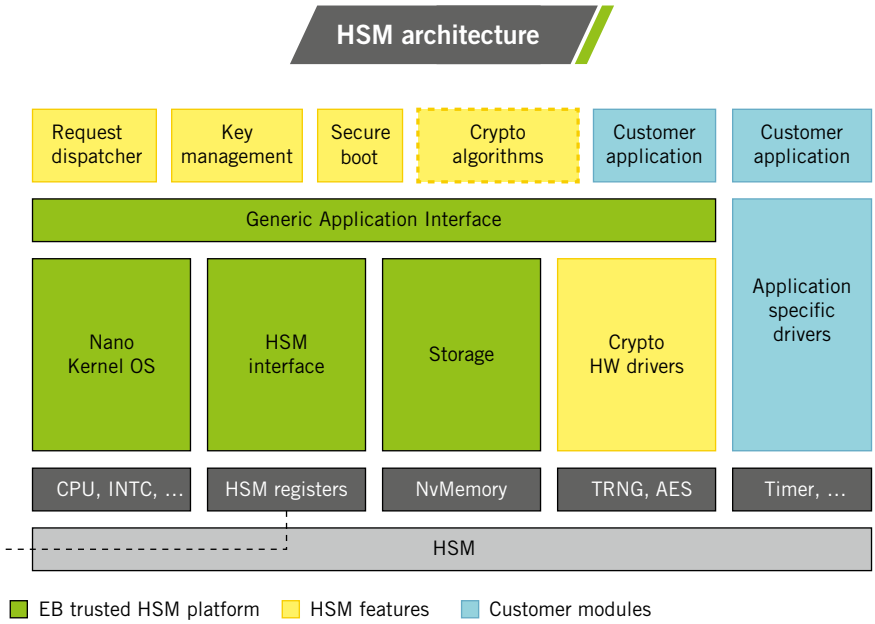



**FIGURE 2** Architecture of an optimized HSM firmware (© Elektrobit)

settings. Another basic application is to check update packages for authenticity and integrity. SecOC (Secure Onboard Communication) or Ethernet-based networks such as TLS (Transport Layer Security) are typically used for network protection within a vehicle. Among other things, both concepts ensure the authenticity of data transmitted within on-board communication. SecOC thereby prevents any manipulation of data packets, man-in-the-middle attacks, or other attack scenarios. To prevent any unauthorized access by hackers to the CAN bus, the SecOC module adds a Message Authentication Code (MAC) to every data block transmitted on the internal bus. To prevent any manipulation due to intercepted data blocks, the cryptographic calculation takes account of a time-dependent component that documents the up-to-dateness of the message.

A central point such as a gateway ideally has an IDPS (intrusion detection and prevention system) that detects suspicious behavior and, depending on the configuration, can forward it to a backend system for further evaluation or, if necessary, directly takes remedial action.

Mechanisms to connect to the outside world also include "classic" solutions and processes from client-server communication, such as TLS (Transport Layer Security), certificate-based authentication, and encryption. Furthermore, specifically hardened communication stacks are used so that the data collected in the vehicle can be securely sent to an automotive security operations center for further evaluation and updates can be received. Messages regarding communication patterns classified as suspicious in the vehicle are collected in the security operations center where they can be evaluated and combined into a fleet-wide image.

In terms of IDPS, protecting the connection to the outside world, and the automotive security operations center, EB works closely with the colleagues from Argus.

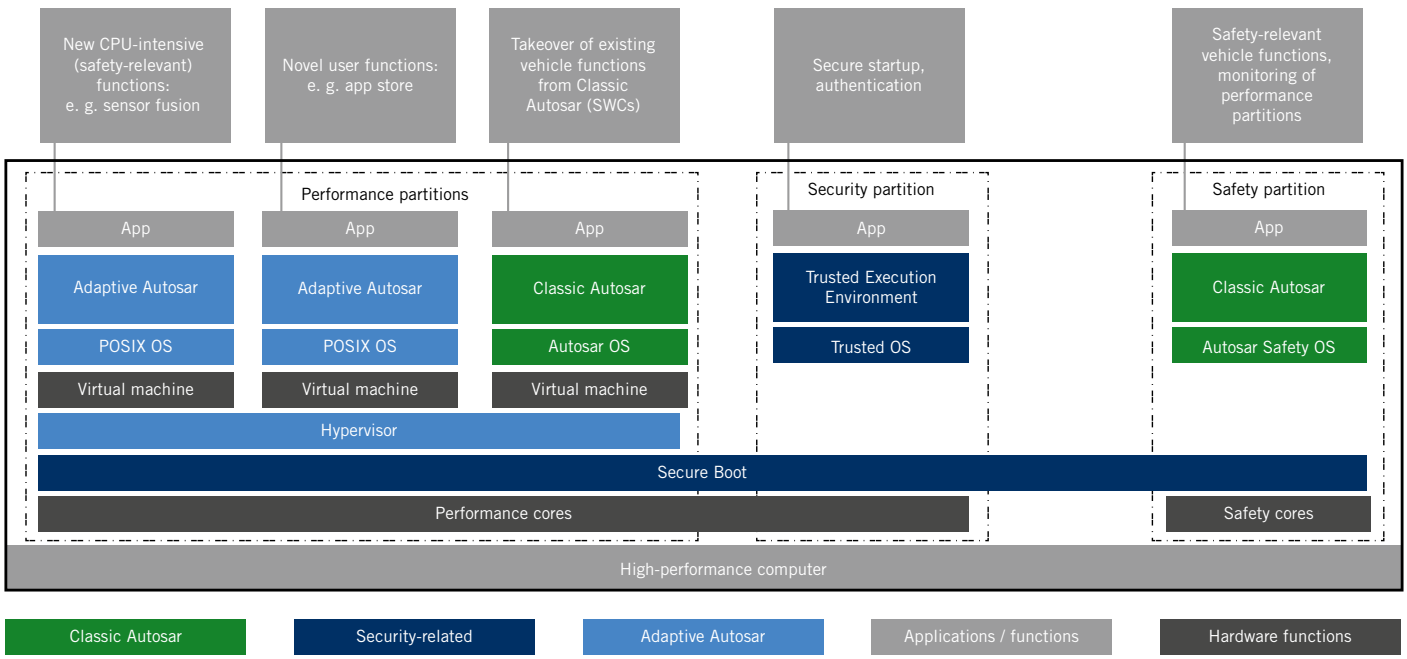



**FIGURE 3** Architecture of a central control unit with performance and safety cores (© Elektrobit)

## SECURITY MEASURES USING THE EXAMPLE OF OTA SOFTWARE UPDATES

Wireless updates allow car makers to offer "upgradeable" cars. As a result, vehicles can be provided with regular function updates, and new functions can be offered over the entire life cycle. Customers of automobile manufacturers are accustomed to OTA software updates from their smartphones and other consumer electronic devices. In the future, they will no longer be willing to take their vehicles to the garage for the sole purpose of having a software update installed.

Based on the security architecture and concepts roughly outlined above, Elektrobit protects the entire update process, from starting the system and receiving the update data over the air to installing the update, **FIGURE 4**. The integrity of the in-vehicle system environment is ensured by a secure boot mechanism that loads and runs only authenticated software components. Verification takes place simultaneously with software execution in order to minimize loading and start-up times. OEM-specific requirements can be seamlessly integrated.

An end-to-end encrypted communication connection between the backend and on-board components as well as encrypted storage of the data in both the backend and the vehicle make sure that the update data is securely transmitted and stored. In the vehicle, the boot loader, which is independent of the applications' program code, ensures a secure environment for installing the update. The safeguards already described are also used to authenticate update packages and to actually install the updated software. During these processes, the Secure Diagnostics system module monitors communication between the diagnostic client and the relevant ECUs. The OEM can choose between different authentication methods, such as challenge-response or token-based authentication.

Update functions for the connected vehicle must be reliably organized and executed securely so that they protect the vehicle over its entire life cycle.

EB's update service EB cadian Sync enables manufacturers to quickly respond to current threats and wirelessly distribute and install security patches to eliminate vulnerabilities of their fleets worldwide. This allows automobile manufacturers to continuously provide safety and security functions of cars in the field with software updates for all ECUs used in the vehicle. In most cases, it is therefore no longer necessary to visit a garage. Moreover, the fleet size is irrelevant to campaign management.

To make the entire update process as simple and uncomplicated as possible for car makers or service providers, EB cadian Sync offers a scalable and flexible full-service solution. Depending on the OEM's specifications, it contains the cloud or backend environment required to prepare, manage, and implement the update throughout the entire life of the vehicle. Within an update rollout, several ECUs and/or the infotainment system of the vehicle can also be updated at the same time. The only essential requirement the relevant ECUs must meet is to support standardized diagnostics protocols and the necessary basic mechanisms for secure updates.

EB cadian Sync supports both existing and new vehicle architectures based on Autosar Adaptive. In conjunction with OTA updates, Autosar Adaptive provides, in a standardized manner, key functions for specifically updating functions and components. While Autosar Classic normally required a full update of the application software, the modular architecture of Autosar Adaptive supports both partial updates that update only individual blocks of an application and delta updates where the target application is patched to the new software version.

In both cases, an update master receives the update data sent over the air from the connectivity client and then specifically updates the individual software components.

## LEGAL REQUIREMENTS FOR AUTOMOTIVE SECURITY

Special requirements for automotive security are not only due to technical reasons. Legislators and industry associations in industrialized countries are currently developing regulations to safeguard automotive cyber security. For example, already in 2017, the US House of Representatives passed the "Self-drive Act" that specifies cyber security and privacy provisions for highly automated and autonomous driving. It requires vehicle manufacturers to have a cyber security plan to identify and prevent attacks or incorrect software commands. In addition, car makers must identify vulnerabilities and, where necessary, eliminate them through software updates. In March 2017, the German Bundestag passed the amendment to the German Road Traffic Act. It specifies initial rules for storing certain vehicle data for liability purposes. The specific

### Required parts for a OTA software update solution

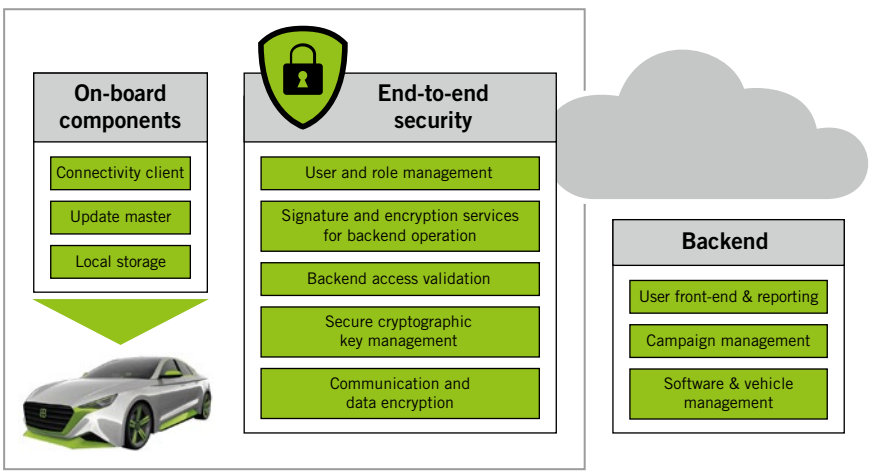



**FIGURE 4** An end-to-end encrypted communication link between backend and on-board components is critical for OTA updates (© Elektrobit)

provisions for automotive cyber security are currently being developed in collaboration with stakeholders from the automotive industry, with the aim of preserving a global focus.

The legal requirements are one building block; however, they only relate to selected areas and naturally lag behind threats. It is therefore crucial to consider security as a fundamental building block for system design right from the start. In addition, measures must be designed such that they prevent as many threats as possible from the outset while identifying unpredicted behavior and ultimately respond accordingly to such situations – from the start of a vehicle's life to its end.

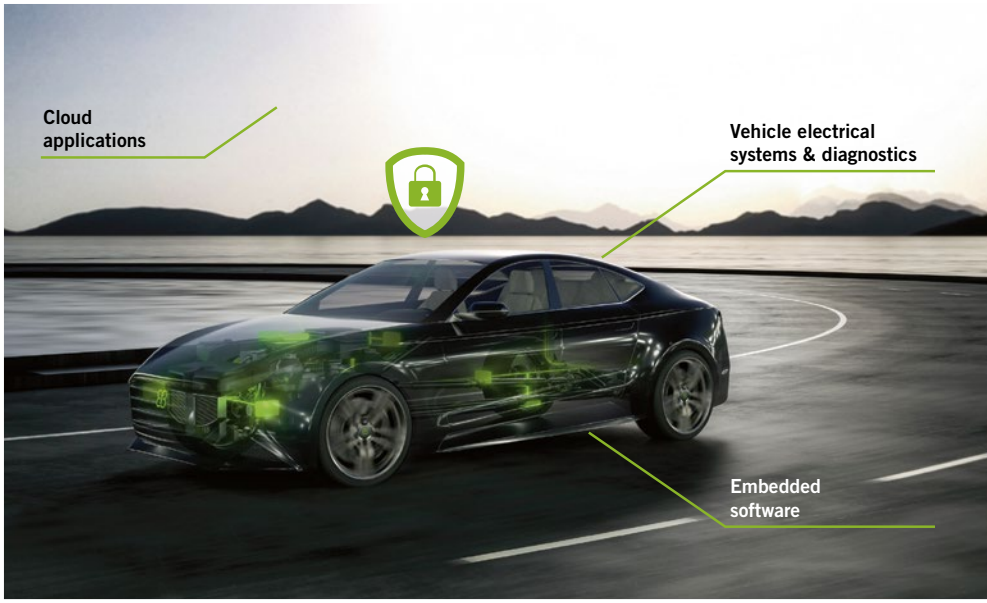



**FIGURE 5** The vehicle in the network (© Elektrobit)

## SOLUTIONS FOR CONNECTED VEHICLES THAT ARE SAFE, SECURE, AND ALWAYS UP TO DATE

Connecting vehicles enables many new and exciting automotive functions, with many possibilities and benefits for both drivers and car manufacturers. For example, new vehicle functions can be provided wirelessly through software updates – even to vehicles that are already on the road. In the context of fully automated driving, connectivity will be an essential, legally required feature.

There is no single solution to preventing cyber attacks. Cyber security solutions are always assessed in terms of their effectiveness, i.e., the extent to which they make potential attacks difficult. Automotive security is not an additional function but a holistic technical concept that covers the entire life cycle and value chain of a vehicle. A comprehensive security solution that considers all the elements involved plays a key role in this concept. The collaboration with its parent company, Continental, enables EB to complement the holistic software solution by appropriate hardware. If requested, Elektrobit provides a complete solution for secure connectivity and over-the-air software updates with the required end-to-end security, **FIGURE 5**.