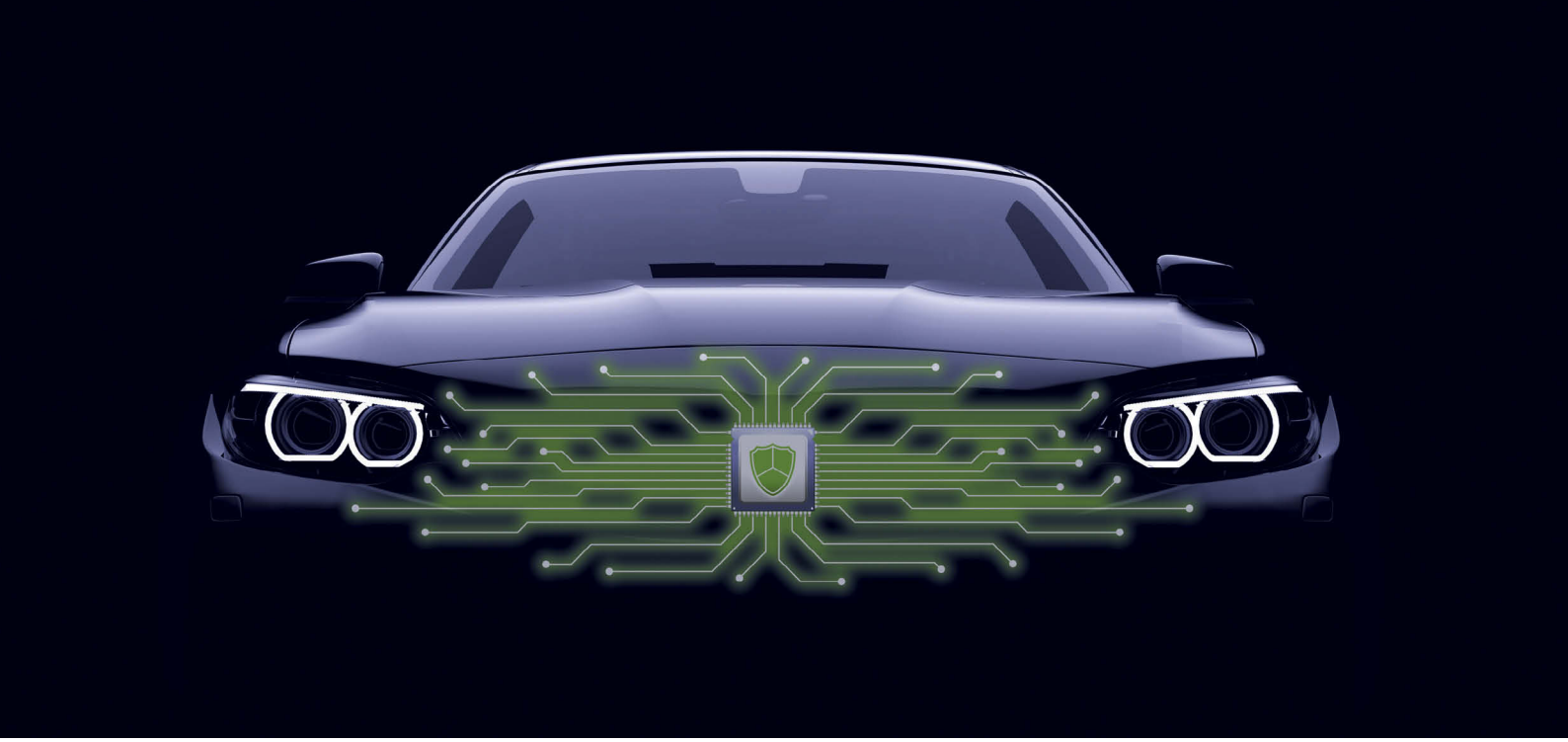

Leistungsschub für Hardware-Security-Module

Neue serviceorientierte HSM-Software sichert künftige Bordnetzarchitekturen

In Fahrzeugarchitekturen der Zukunft wird ein Gutteil der Software auf Domänencontrollern zentralisiert und Automotive Ethernet ermöglicht breitbandige Onboard-Kommunikation. Das erfordert neue Ansätze in der IT-Sicherheit. Hardware-Sicherheitsmodule (HSMs) der neuen Generation werden zum zentralen Baustein. Denn sie vereinen Multi-App-Fähigkeit mit Echtzeitkommunikation.

Schon bald sollen Vehicle Computer Fahrzeugdomänen und ihre softwaregesteuerten Funktionen zusammenführen. Die Steuergeräte in der Peripherie entwickeln sich zunehmend zu Eingabe-/Ausgabegeräten, deren eigentliche Applikation in der Rechnerebene stattfindet. Die Vorteile für den OEM sind weitreichend: Die IP verlagert sich auf die Zentralrechner. Die Komplexität von E/E-Architekturen sinkt ebenso wie der Engineering-Aufwand. Statt für jede Fahrzeuggeneration spezifische Steuergeräte samt Software einzukaufen, können OEMs die Entwicklung und das Miteinander der Software-Applikationen auf den Vehicle Computern bündeln – und so Zeit und Kosten sparen.

Allerdings nimmt mit der Zentralisierung die Onboard-Kommunikation zu. Statt der dezentralen Verarbeitung in Steuergeräten müssen Daten im Domänencontroller gesammelt, verarbeitet und im Fahrzeug verteilt werden. Weil dafür oft Echtzeitanforderungen gelten, wird der Datenverkehr per Automotive Ethernet laufen. Daneben bleibt es in Subnetzen bei der Signalübertragung per CAN-Bus. Die IT-Sicherheit muss an diese hybriden Architekturen angepasst werden.

Security-by-Design

Mit Blick auf die zunehmende Vernetzung sollten Security-by-Design und Update-by-Design in den hybriden Bordnetzen fest verankert sein. Zumal die angelegte Entkopplung von Hard- und Software sowie die Verlagerung vieler Software-Applikationen auf zentrale Rechner dafür neue Möglichkeiten eröffnet. Denn auch IT-Sicherheitsfunktionen lassen sich in den zentralisierten Bordnetzen zentral verwalten. Gleichzeitig muss der Schutz der Steuergeräte in der Peripherie gewährleistet bleiben.

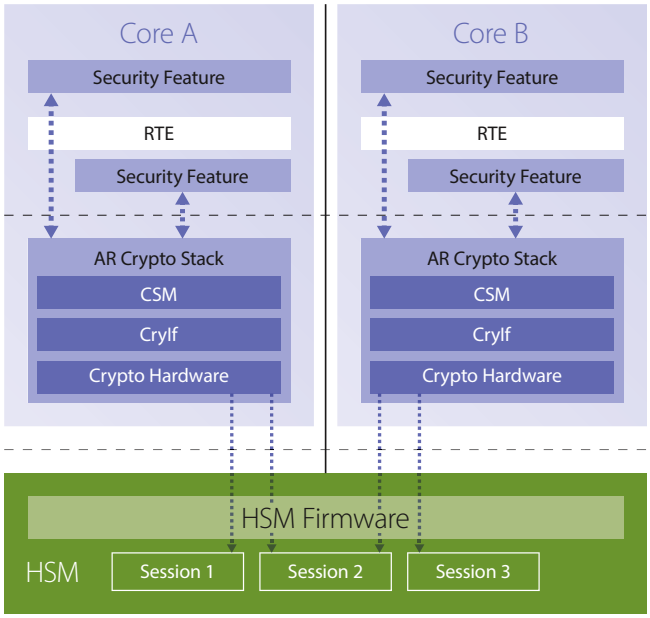

Bild 1: Anfragen mehrerer Host-Cores werden von der HSM-Firmware in parallelen Sessions verarbeitet.

Für eine rundum abgesicherte Onboard-Kommunikation (SecOC) sind unter anderem Hardware-Security-Module vonnöten. Diese helfen, die Authentizität sämtlicher hier zusammenlaufender Daten sicherzustellen und verhindern, dass sich Angreifer über den Umweg sicherheitsrelevanter ECU-Schnittstellen Zugang zur zentralen Recheneinheit oder sogar zum Bordnetz verschaffen. Doch die Herausforderungen in zentralisierten Bordnetzen gehen darüber hinaus: Wo zentrale, oft in viele virtuelle Maschinen partitionierte Vehicle Computer Software-Anwendungen und Funktionen mehrerer Steuergeräte übernehmen, steigen auch die Anforderungen an die Security-Bausteine. Eine neue Generation von Hardware-Security-Modulen ist bereits darauf vorbereitet.

Job-Bevorrechtigung und Echtzeit-Betriebssystem

Bekanntlich sind bei HSMs die IT-Sicherheitsfunktionen auf dem Mikrocontroller der Recheneinheit in einem HSM-Core physikalisch gekapselt. Dort werden sie per HSM-Software-Stack aktiviert und betrieben. Der Host-Controller des Rechners kann sich so seinen eigentlichen Aufgaben widmen, während der HSM-Kern Security-Anforderungen abarbeitet: Secure Onboard Communication, Runtime Manipulation Detection, sicheres Booten, Flashen, Loggen oder Debuggen. Damit sind HSMs deutlich leistungsstärker als rein softwaregestützte IT-Sicherheitslösungen.

Werden Software-Anwendungen und ECU-Funktionen auf Vehicle Computern zusammengezogen, dann ist absehbar, dass mitunter viele Applikationen gleichzeitig um die Security-Funktionen des HSM konkurrieren. In dem Fall muss das HSM die nötigen IT-Sicherheitsfunktionen bereitstellen und die Datenströme mehrerer Anwendungen in Echtzeit bewältigen. Klassische HSMs stoßen hier an Grenzen; softwaregestützte Security-Lösungen erst recht. Doch eine neue Generation von Hardware-Security-Modulen mit Realtime-Betriebssystem und intelligentem, flexiblem Session-Konzept ist den Anforderungen gewachsen.

Multi-Core-/Multi-Application-Support

Stellen in künftigen Architekturen mehrere Kerne parallel Anfragen, dann sorgt die Firmware der neuen Generation dafür, dass der HSM-Core diese in bis zu 16 parallelen Sessions verarbeitet. Wobei die genaue Anzahl der Sessions in den modernen HSM-Software-Stacks konfigurierbar ist. Das Geheimnis dieses Multi-Core- und Multi-Application-Supports liegt in der speziellen Architektur des HSM-Firmware-Treibers. Diese erlaubt es verschiedenen virtualisierten Applikationen, den Treiber jeweils eigenständig zu integrieren. Das ebnet den Weg zur unabhängigen Entwicklung verschiedener Softwareteile: Bei der Integration wird im „Linker"-Schritt sichergestellt, dass die verschiedenen Instanzen des Treibers eine gemeinsame Struktur im Shared RAM der Hardware nutzen. Hier legt jede Instanz eigene Strukturen (Sessions) an, sodass der Treiber stets mehrere Anfragen der strikt gekapselten Applikationen parallel verwalten kann (Bild 1).

Eine zentrale Security-Komponente ist dabei die Host-to-HSM-Bridge. Als trennendes Element zwischen Hardware-Security und Host übernimmt sie die „Zuflussregelung" zum HSM. Im Bridgeregister wird die Queue der Anfragen aus den Host-Cores so auf- und abgebaut, dass das HSM als limitierte Ressource unter optimaler Auslastung die angeforderten Security-Funktionen schnellstmöglich ausführen kann. Mit der neuen HSM-Software-Generation wird die Multi-App- und Multi-Core-Fähigkeit des HSM real. OEMs können in abschließend getesteter, serienreifer Form darauf zugreifen (Bild 2).

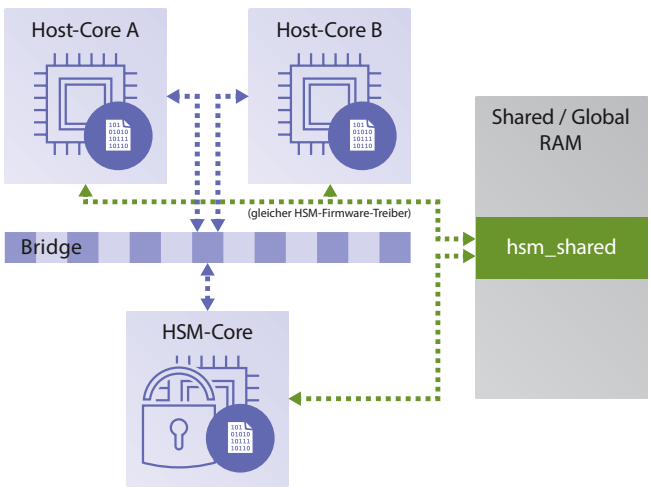

Bild 2: Multi-Core-/Multi-Application-Support – Job Requests werden per Bridgeregister und Shared RAM abgearbeitet.

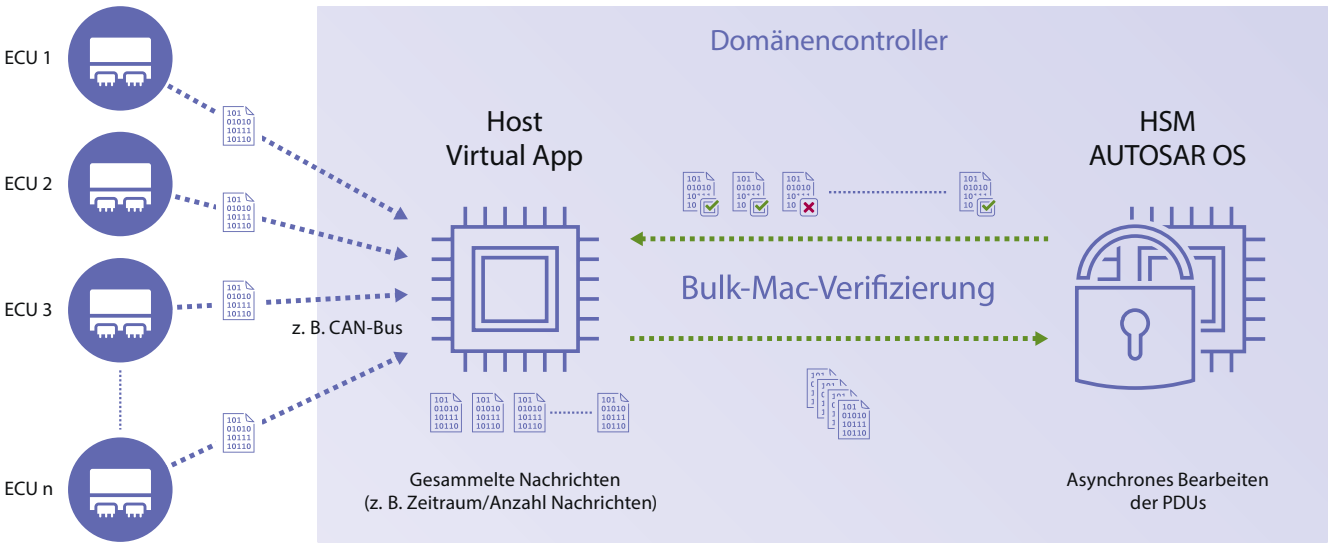

Bild 3: Das Bulk-Mac-Interface sorgt für sichere Echtzeitkommunikation.

Bulk-Mac-Interface sorgt für Echtzeit-Performance

Eine weitere Herausforderung ist die Absicherung der stark zunehmenden Kommunikation. Das Nebeneinander von CAN-Bussen und Automotive Ethernet in den zentralisierten Bordnetzen und der sichere fahrzeuginterne Datenaustausch unter Absicherung aller Kommunikationsprotokolle sind anspruchsvoll. Auch dafür bieten die neuartigen HSMs eine Lösung, obwohl ihr Leistungsvermögen nicht unbegrenzt ist. Grenzen setzt allerdings weniger die Hardware-Crypto-Engine des HSM als das Bridgeregister. Denn Daten lassen sich darüber nicht in beliebiger Menge und Geschwindigkeit austauschen. Abhilfe schafft ein sogenanntes Bulk-Mac-Interface: Der Host sammelt zunächst über einen vorbestimmten Zeitraum sämtliche Nachrichten und stellt diese dann über das Bridgeregister en bloc als Anfrage an das HSM ein. So genügt ein(!) einziger Datentransfer. Die HSM-Firmware prozessiert auf einen Schlag alle gesammelten Nachrichten auf der HSM-Hardware-Einheit und übermittelt die Ergebnisse an den Host (Bild 3).

Der Performancegewinn ist eklatant. Selbst wenn der einzelne Datentransfer zwischen Host und HSM nur 10 µs dauert, summiert sich der Verzug bei hundert Nachrichten auf 1 ms. Für Realtime-Systeme ist dies problematisch. Per Bulk-Mac-Interface lassen sich diese hundert Nachrichten in einem Hundertstel der Zeit abhandeln. Für OEMs, die Netzwerke mit zentralen Computern und Domänencontrollern aufsetzen und dabei viele PDUs definieren, bietet ein Bulk-Mac-Interface also sehr konkrete Vorteile. Es gewährleistet ausreichend schnelle Authentifizierung von großen Mengen unterschiedlicher Nachrichten und erhält so die sichere Echtzeitkommunikation im Fahrzeugnetzwerk aufrecht. In der neuen HSM-Software-Generation ist dieses Bulk-Mac-Setup bereits serienreif integriert.

Zukunftssichere Hardware-Security-Firmware

Bordnetze wandeln sich zu zentralisierten Plattformen, in denen die Entkopplung von Hardware und Software voranschreitet. Für die IT-Sicherheit solcher Plattformen kommt Hardware-Security-Modulen neuer Prägung eine zentrale Rolle zu. Denn sie schützen nicht nur die Datenströme zwischen weiterhin CAN-Bus-dominierter Peripherie und zentralen Controllern vor Zugriff und Manipulation (SecOC). Sondern sie sind dank Multi-Core- und Multi-App-Fähigkeit und Bulk-Mac-Interface auch in der Lage, Security-Use-Cases auf oberster Netzwerkebene abzudecken und laufende Software-Anwendungen mit hoher Datenlast und unter Echtzeitanforderung abzusichern.

Mit Blick auf die zunehmende Konnektivität und den Trend zum automatisierten Fahren setzen OEMs vermehrt auf eigene, spezifische Security-Standards für E/E-Architekturen. Hardware-Security-Firmware der neuen Generation lässt sich in dedizierten OEM-Produktvarianten abbilden – und flexibel in zentrale Sicherheitskonzepte integrieren. Sie läuft auf den Mikrocontrollern neuester Bauart und stellt ihren Host-Treiber als Source Code bereit. Das eröffnet OEMs und Tier 1s eine Fülle an Möglichkeiten zur Wiederverwendung und Anpassung. Dank dieser Flexibilität und ihrer Performance sind Hardware-Security-Module mit Firmware neuester Prägung ein fundamentaler Baustein für die Absicherung zentralisierter, hybrider Bordnetze der Zukunft. ■

Autoren

Dipl.-Ing. Tobias Klein ist Lead Product Owner HSM bei ESCRYPT.
Dr. Frederic Stumpf ist Head of Product Management Cybersecurity Solutions bei ESCRYPT.