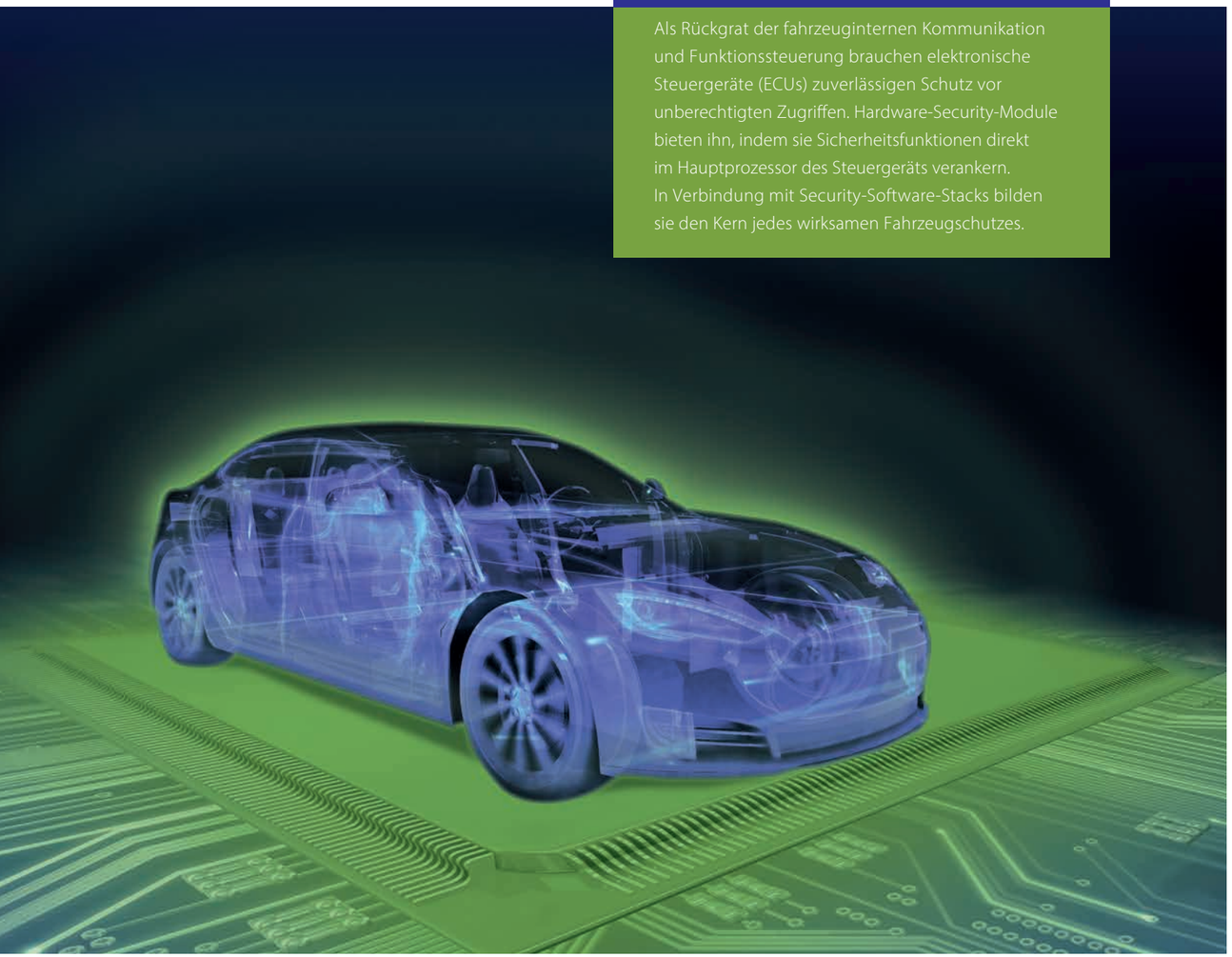
Automotive Security von innen heraus

Schutz durch Hardware-Security-Module (HSM) im ECU-Hauptprozessor



Als Rückgrat der fahrzeuginternen Kommunikation und Funktionssteuerung brauchen elektronische Steuergeräte (ECUs) zuverlässigen Schutz vor unberechtigten Zugriffen. Hardware-Security-Module bieten ihn, indem sie Sicherheitsfunktionen direkt im Hauptprozessor des Steuergeräts verankern. In Verbindung mit Security-Software-Stacks bilden sie den Kern jedes wirksamen Fahrzeugschutzes.

Wenn Chip-Tuner in Antriebssteuergeräte eindringen und Systemparameter verschieben, sind ihnen Lärm- und Umweltschutz oft völlig egal. Viel beunruhigender ist es allerdings, dass sie überhaupt auf elektronisch gesteuerte Fahrzeugsysteme zugreifen können.

Nicht auszudenken, was böswillige Eingriffe in Antriebs- und Fahrwerksteuergeräten auslösen können. Gerade im vernetzten Fahrzeug kann jedes Steuergerät im Bordnetz zum Angriffsziel werden. Damit Unbefugte weder Software manipulieren können noch kritisches Schlüsselmaterial in die Hände bekommen, brauchen moderne Fahrzeuge zuverlässige IT-Sicherheitsmechanismen, die sie von der Außenwelt abschirmen. Genau das leisten Hardware-Security-Module (HSM), mit denen Sicherheitsfunktionen direkt in ECUs implantiert werden.

Automotive-spezifische Hardware-Security-Module

Beim HSM handelt es sich um eine Hardwarekomponente, die Sicherheitsfunktionen physikalisch kapselt. Als integrierte Chips sind sie speziell für IT-Sicherheitsanwendungen ausgelegt. Typischerweise verfügen sie über einen eigenen CPU-Core, verschiedene Datenspeicher (z. B. RAM, ROM oder Flash) und kryptografische Hardwarebeschleuniger. Bei der Verwendung im Fahrzeug kommen spezifische Anforderungen hinzu. Der Kostendruck erfordert eine hocheffiziente Integration des HSM. Sichere Schnittstellen zwischen ECU-Anwendung und HSM sind ebenso zu gewährleisten wie Debug- und Testing-Schnittstellen für die Analyse von Fehlfunktionen. Auch sollen HSM kryptografische Informationen mit minimaler Latenz verarbeiten und die automotive-typische Temperaturbeständigkeit aufweisen.

Solche Hardware-Security-Module mit automotive-gerechter Architektur bieten heute mehrere führende Chip-Hersteller an, darunter Infineon, ST Microelectronics, Renesas und NXP. Die Grundidee: Mithilfe des eigenen Core-Prozessors stellen die HSM alle nötigen IT-Security-Stammfunktionen für Automotive-Use-Cases bereit. Sei es eine AES-128-Bit-Hardware-Engine, ein Zufallszahlengenerator (TRNG) zum Generieren von Schlüsselmaterial, das hardwaregeschützte Speichern kryptografischer Schlüssel, seien es Flash- und Debug-Funktionen oder der eigene vom Systemspeicher unabhängige HSM-RAM (siehe Bild 1).

Passgenaue Security-Software und Echtzeitkommunikation

Wirklich zum Leben erweckt wird ein solches HSM erst durch einen Secure-Software-Stack. Wenn das HSM der „Zellkern" der IT-Security im Fahrzeug ist, dann ist die HSM-Security-Software ihr „genetischer Code". ESCRYPT liefert ihn in Form der Security-Firmware CycurHSM – passgenau ausgelegt auf Automotive HSM verschiedener Anbieter. CycurHSM verknüpft die vorhandene Hardware-Security-Peripherie mit den jeweiligen Applikationen von HSM und Host-Controller. Auch bestückt die Firmware das HSM mit einer umfassenden kryptografischen Bibliothek inklusive symmetrischer und asymmetrischer Verschlüsselungsmechanismen sowie weiterer HSM-basierter Security- Funktionen. Auch die nötigen AUTOSAR- und nicht-AUTOSAR-kompatiblen Schnittstellen, um HSM in typische Fahrzeugsteuergeräte zu integrieren, bringt CycurHSM mit.

Kernelement der Software-Architektur ist ein Echtzeitbetriebssystem. Dieses ist spezifisch auf Automotive-ECUs ausgerichtet,

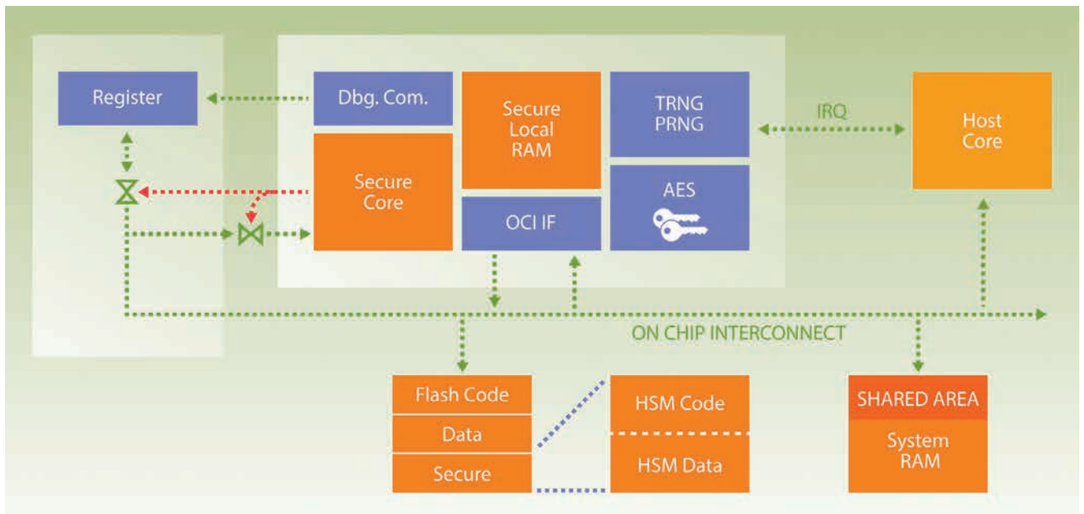


Bild 1: Hardware-Architektur des Hardware-Security-Moduls (HSM)

nach ISO 26262 zertifiziert und es unterstützt Echtzeitfunktionen des HSM – etwa eine sichere fahrzeuginterne Echtzeitkommunikation. Das Betriebssystem arbeitet mit minimalem Laufzeit-Overhead und ist MISRA-C-konform. Ein Session-Manager sorgt dafür, dass Tasks gemäß ihrer Priorität abgearbeitet werden. So hat die Validierung neuer Nachrichten auf dem Fahrzeugbus Vorrang vor nicht zeitkritischen Operationen. Hinzukommt ein Keystore-Manager, welcher den Zugriff auf sowie das Generieren, Speichern und Löschen von Schlüsselmaterial im HSM regelt und dabei symmetrische und asymmetrische Schlüssel unterschiedlicher Länge berücksichtigt. Die kryptografische Bibliothek (CycurLIB) stellt die kryptografischen Primitive (ECC, RSA) bereit und greift dafür auf die Kryptografiebeschleuniger des HSM zurück. Bei Bedarf lässt sich unter Zugriff auf die Kryptobibliothek auch eine SHE-Emulation auf dem HSM ausführen, um erweiterte automotive-spezifische Anforderungen (SHE+) zu erfüllen. Obendrein sichern spezifische HSM-Treiber die Kommunikation zwischen HSM und Host-Prozessor, wobei ein AUTOSAR-kompatibler Cryptographic Service Manager (CSM) direkt an der Schnittstelle zum HSM dafür sorgt, dass AUTOSAR-Applikationen jederzeit auf das Modul zugreifen können (siehe Bild 2).

- Leistungsfähige Hardware-/Software-Codesign-Plattform für kundenspezifische Applikationen mit Hochleistungs-Verschlüsselungsanforderungen
- Ermöglicht einfache Kundenintegrationen durch standardisierte Schnittstellen zum HSM
- Dank modularer Struktur bedürfnisgerecht anpassbar und voll programmierbar
- Multi-Core-Unterstützung

Auf dieser Grundlage unterstützt der HSM-Software-Stack ein breites Spektrum an Security-Use-Cases. Er liefert eine standardisierte Schnittstelle, über die – basierend auf starker Kryptografie – entweder im HSM selbst oder im Zusammenspiel mit dem Host-Prozessor vielfältige IT-Sicherheitsfunktionen umsetzbar sind. Das fängt beim sicheren Booten an, also der Überprüfung des hinterlegten Codes im Flashspeicher bei jeder ECU-Initialisierung, geht mit der Runtime Manipulation Detection und sicherem Flashen samt Authentifizierung der Absender von Softwaredownloads weiter und reicht bis zu einer Secure-Log-Funktion zur durchdachten Dokumentation sicherheitskritischer Ereignisse. Grundprinzip ist

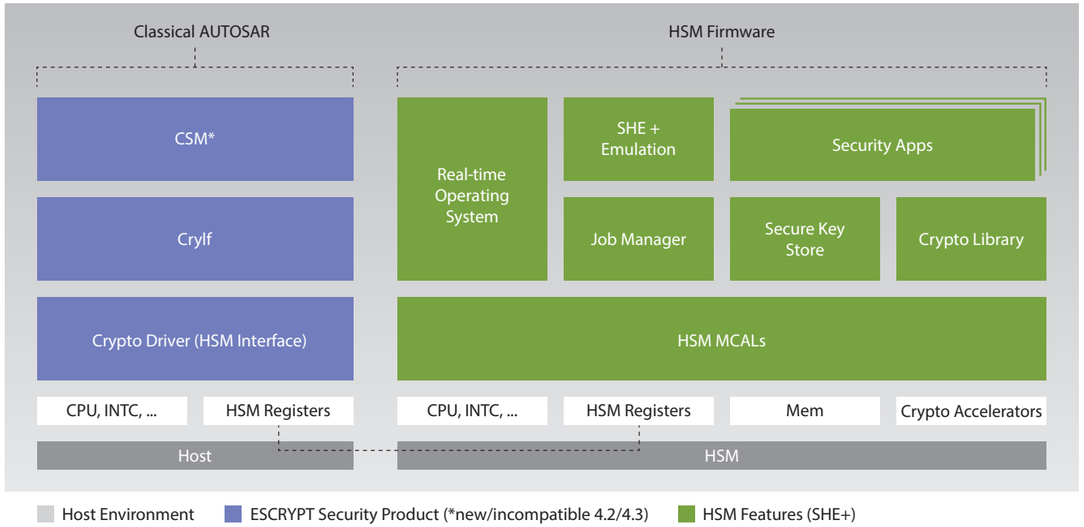


Bild 2: Software-Architektur des Hardware-Security-Moduls (HSM)

Leicht zu implementieren und multifunktional

Verglichen mit rein softwaregestützten Lösungen ist ein Hardware-Security-Modul deutlich leistungsstärker. Da die Sicherheitsfunktionen physikalisch gekapselt sind, kann sich der Host-Controller der ECU ganz den eigenen Aufgaben widmen. In Verbindung mit der HSM-Security-Software steht eine „schlüsselfertige" Lösung bereit, die zahlreiche Vorteile bietet:

jeweils die wechselseitige Authentifizierung von anfordernder Instanz und HSM. Dies gilt auch für das sichere Debuggen. Es schützt die ECU vor unberechtigtem Zugriff über den Debug-Port und erlaubt zugleich den autorisierten Zugriff zur Korrektur von Softwarefehlern. Die Hoheit über die Kommunikation und Authentifizierung liegt auch hier beim HSM.

Neue HSM-Firmware-Generation

Da Hard- und Software-Entwicklung im Bereich der HSM schnell voranschreiten, verfügen heute immer mehr Mikrocontroller für ECUs serienmäßig über ein automotive-spezifisches Hardware-Security-Modul. ESCRYPT entwickelt im gleichen Atemzug die HSM-Software-Stacks (CycurHSM) weiter. Deren neueste Generation bietet noch differenziertere und komfortablere Möglichkeiten, um individuell ausgelegte IT-Sicherheitsfunktionen in ECUs zu implementieren: Die neuartige HSM-Firmware erlaubt eine einfache Konfiguration per Applet-Manager sowie die Aktivierung einzelner Sicherheitsmerkmale mittels Variant-Management-System. Zudem verfügt die ASPICE-konforme Software über eine flexible Keystore-Architektur.

Um vernetzte Fahrzeuge und ihre zunehmend automatisierten Fahrfunktionen auch in Zukunft abzusichern, ist ganzheitlicher Schutz gefragt. Er muss an neuralgischen Punkten der Vernetzung ansetzen; etwa per Intrusion-Detection-System, Automotive Firewall und sicheren Over-the-Air-Software-Updates oder Secure V2X. Und er sollte IT-Sicherheitsfunktionen schon in den Elementarteilchen digitaler Fahrzeugfunktionen verankern – den Mikroprozessoren der einzelnen Steuergeräte. Hardware-Security-Module sind dazu in der Lage. Ihnen gehört die Gegenwart – und erst recht die Zukunft der Automotive Security. ■

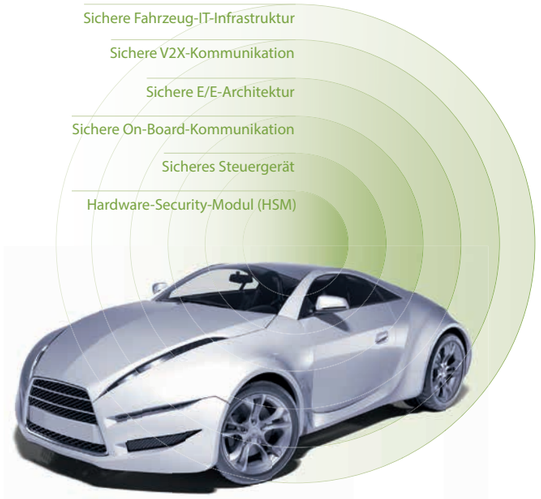


Bild 3: Hardware-Security-Modul (HSM) als Nukleus der Automotive Security

Autor

Dr. Frederic Stumpf ist Leiter Product Management bei **ESCRYPT**.

ESCRYPT zum Innovator 2018 gekürt

Der renommierte Wirtschaftsverlag **brand eins** zählt ESCRYPT zum Kreis der innovativsten deutschen Unternehmen. Unter den Mittelständlern im Bereich „Technologie & Telekommunikation" belegte ESCRYPT im diesjährigen Ranking einen Spitzenplatz und erhielt die Auszeichnung **„Innovator des Jahres 2018".**

Insgesamt 25.000 Experten waren aufgefordert, anhand spezifischer Kriterien aus insgesamt mehr als 3.400 Unternehmen ihre Innovationsführer zu benennen. ESCRYPT wurde dabei von den Befragten in allen drei Innovationsbereichen – bei Produkten und Dienstleistungen, Prozessinnovationen und der Unternehmenskultur – überdurchschnittlich oft empfohlen. **„Wir freuen uns sehr über diese Auszeichnung, sehen sie aber auch als Ansporn"**, betont Geschäftsbereichsleiter Dr. Uwe Müller. **„Erfindergeist soll auch weiterhin unsere treibende Kraft bleiben."** ■

brand eins Thema
2018
INNOVATOR DES JAHRES