escrypt
SECURITY. TRUST. SUCCESS.

INTERVIEW

Zukünftige Security-Standards erfolgreich meistern

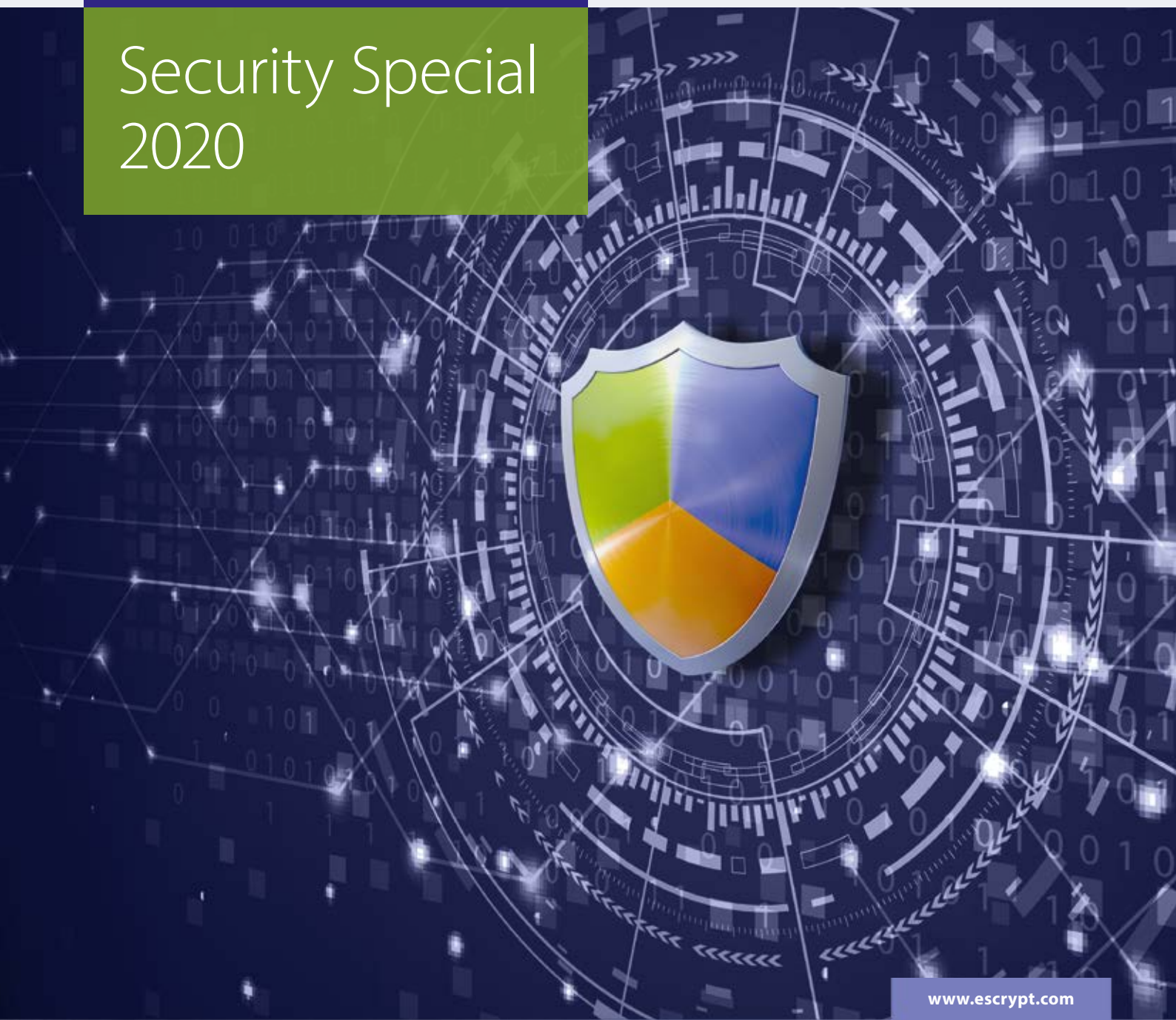
ANGRIFFSERKENNUNG

Automotive Firewall und IDS im Zusammenspiel

HARDWARE-SECURITY-MODUL

HSM-Firmware der nächsten Generation

# Security Special 2020



www.escrypt.com

# „Cybersecurity wird Voraussetzung für die Typzulassung“

## Dr. Moritz Minzlaff über Automotive Security als strategische Aufgabe

**Steigende Security-Anforderungen fürs Fahrzeug manifestieren sich gerade in einer Welle neuer Standardisierungen und Regularien. Im Interview erläutert Dr. Moritz Minzlaff, Senior Manager bei ESCRYPT in Berlin, worauf sich die Automobilindustrie einstellen muss.**

***Herr Doktor Minzlaff, die Schaffung verbindlicher Standards und Regularien im Bereich der Automotive Security hat inzwischen richtig Fahrt aufgenommen. Welche Entwicklungen verdienen hier besonderes Augenmerk?***

Es gibt zwei Initiativen, die im Moment alle gebannt verfolgen: Zum einen die ISO/SAE 21434, die Standards setzt auf der Prozessebene. Zum anderen die Aktivitäten der UNECE WP.29, die Cybersecurity für die Typzulassung von Fahrzeugen zur Voraussetzung machen wird. Beide, UNECE-Regularien und ISO-Vorgaben, werden schon innerhalb der nächsten drei Jahre in Kraft treten. Es bleibt also wenig Zeit, sich darauf vorzubereiten.

***Das heißt, die Informationssicherheit der Fahrzeuge wird in naher Zukunft tatsächlich typzulassungsrelevant?!***

Das ist richtig. Gemäß UNECE-Vorgaben werden die OEMs künftig in Märkten wie der EU oder Japan Fahrzeugtypen nur noch zulassen können, wenn sie eine angemessene Risikobehandlung nachweisen. Die ISO/SAE 21434 ist dann das Puzzlestück in Form gemeinsamer Security-Standards der Automobilindustrie, das über die Hürde hinweg helfen soll. Gleichzeitig entwickeln sich auf regionaler Ebene ständig weitere Regelwerke und Gesetze, die es ebenfalls im Blick zu behalten gilt.

***Welche Herausforderungen kommen da denn jetzt konkret auf die Autohersteller und Zulieferer zu?***

Die große Herausforderung besteht darin, dass Security künftig ganzheitlich über die Lieferkette und den Lebenszyklus angegangen werden muss. Es reicht nicht mehr, zwei oder drei zentrale Steuergeräte mit Security-Funktionen zu versehen. Fahrzeughersteller werden für die gesamte Plattform kritische Elemente identifizieren und absichern müssen – und das bis zum Phase-out. Lifecycle-Management ist daher in Zukunft ein entscheidendes Thema: Wie lässt sich nach Start of Production risikobasiert für einen angemessenen Schutz sorgen? Und zwar für vernetzte Fahrzeuge, die über viele Jahre im Feld einer sich kontinuierlich ändernden Bedrohungslandschaft ausgesetzt sind.

***Was sollte ich als OEM oder Zulieferer denn jetzt schon tun, um den Schutz von Fahrzeugen in meinem unternehmerischen Handeln und meiner Organisation nachhaltig zu verankern?***

Sie sollten aus zwei Richtungen aktiv werden. Zum einen sollten Sie den Security-Bedarf ihres Produkts ermitteln: Fahrzeuge und Komponenten mit unterschiedlichem Vernetzungsgrad, unterschiedlicher Funktionalität, unterschiedlicher Safety-Relevanz und unterschiedlichem Grad des automatisierten Fahrens brauchen jeweils angepasste Schutzmaßnahmen. Um das so identifizierte Security-Niveau zu erreichen, müssen Sie alle Beteiligten einbinden: Von Entwicklung und Produktion über die Qualitätssicherung bis hin zu Vertrieb und Kundenkommunikation müssen im eigenen Unternehmen und entlang der Lieferkette Verantwortlichkeiten und Rollen klar definiert werden.

Gleichzeitig können Sie eine „Bestandsaufnahme“, also ein klassisches Audit oder Assessment durchführen. In welchen Bereichen sind Sie gut aufgestellt, welche Teile der künftigen regulatorischen Anforderungen erfüllen Sie bereits? Auf welche vorhandenen Prozesse können Sie aufbauen? Solch eine Gap-Analyse zeigt auf, wo Investitionen in die Weiterentwicklung des Themas Security die größte Wirkung entfalten.

***Ist es sinnvoll, sich hier einen Security-Spezialisten wie ESCRYPT an die Seite zu holen?***

Ja, denn unser unabhängiger Blick und unser globales, branchenweites Know-How ist die optimale Ergänzung zur hausinternen


**Moritz Minzlaff**
Senior Manager bei ESCRYPT

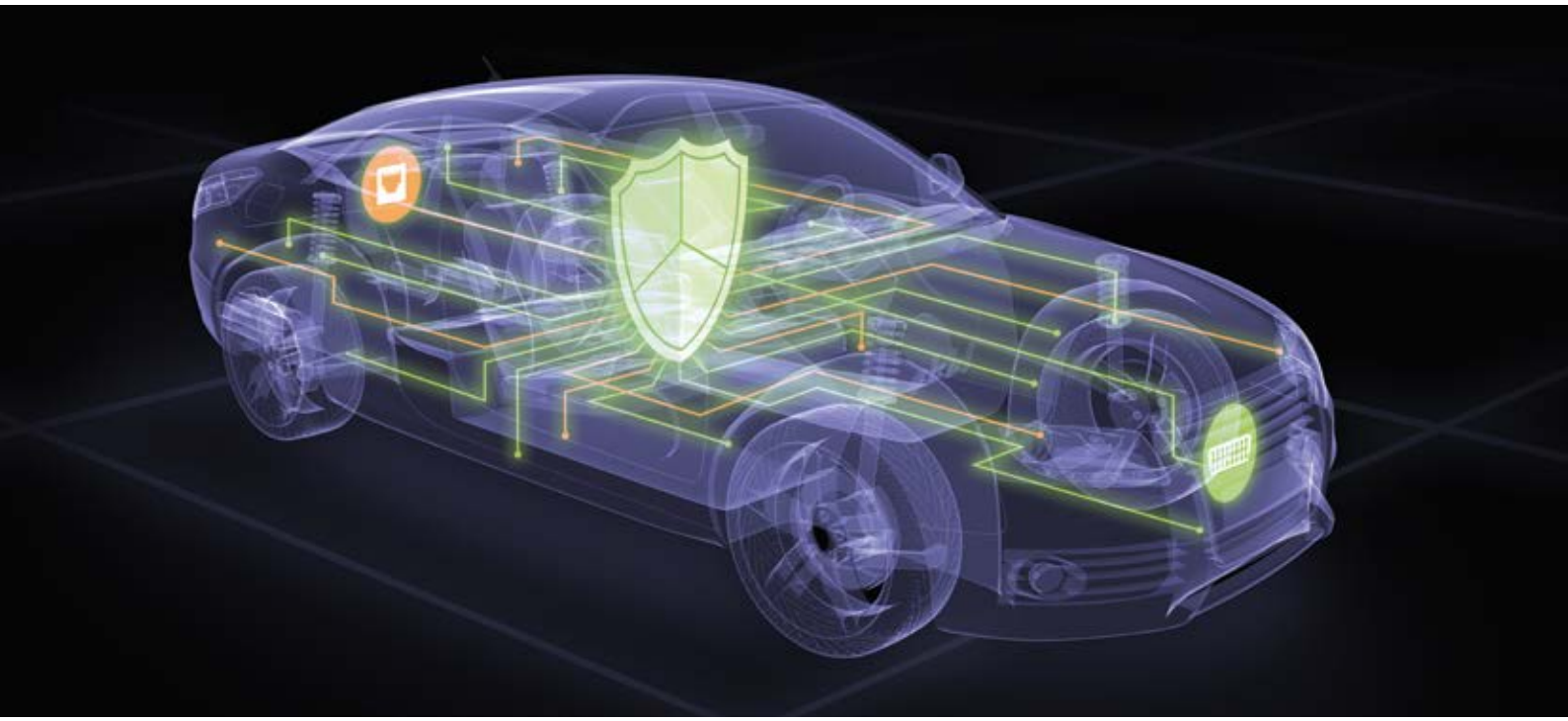
*„Der kontinuierliche Schutz vernetzter Fahrzeuge gelingt nur miteinander und ganzheitlich."*

Kompetenz. Der kontinuierliche Schutz vernetzter Fahrzeuge gelingt nur miteinander und mit einem ganzheitlichen Ansatz. Bei ESCRYPT haben wir daher heute bereits klassische Enterprise-IT-Sicherheit mit eingebetteter Sicherheit zusammengeführt. Denn nur domänenübergreifend vom Fahrzeug über Apps bis hin zur Cloud lässt sich Cybersecurity in Zukunft meistern.

Aufgrund unserer vielfältigen Projekterfahrung mit Herstellern und Zulieferern in allen großen Märkten können wir zudem ein „Benchmarking" bieten. Wir identifizieren genau die Aspekte der gelebten Security-Praxis, die weiterentwickelt werden sollten, und helfen, die notwendigen Investitionen in Cybersecurity zielgerichtet zu bestimmen. Die Zeit ist knapp und das Risiko ist zu groß, die Typzulassung gemäß UNECE-Vorgaben nicht oder nur mit Verspätung oder Kostenüberlauf zu erreichen. Dank tiefer Engineering-Erfahrung wissen wir bei ESCRYPT, wie man Automotive Security am Ende in Serie bringt. All das erhöht die Chance drastisch, die bevorstehenden Herausforderungen erfolgreich zu bewältigen. ■

# Angriffserkennung für hybride CAN-Ethernet-Netzwerke

## Automotive Cybersecurity zielgenau auf beide Welten abstimmen



**Heutige dezentrale E/E-Architekturen werden den vernetzten, automatisierten Fahrzeugen der nahen Zukunft nicht mehr gerecht. Daher werden Vehicle Computer und Automotive Ethernet herkömmliche Steuergeräte und CAN-Busse ergänzen. Solche hybriden Fahrzeug-Netzwerke brauchen Schutz durch zielgenaue Angriffserkennung und Überwachung des Datenverkehrs.**

Bald schon werden Vehicle Computer (VC) und breitbandiges Automotive Ethernet heutige Bordnetze mit ihren dutzenden, durch CAN-, LIN- und FlexRay-Datenbusse verbundenen Steuergeräten ergänzen. Letztere bleiben gefragt, wo es hohe Echtzeitanforderungen und zyklisch wiederkehrende Funktionen umzusetzen gilt. Ansonsten übernehmen mikroprozessorbasierte, in Virtual Machines partitionierte Zentralrechner. Denn sie sind den Herausforderungen vernetzter, automatisierter Fahrzeuge besser gewachsen.

Doch wie lassen sich die hybriden CAN-Ethernet-Architekturen und deren Datenprozesse effektiv absichern? Grundsätzlich bleibt es bei zwei Prinzipien: Abschirmung der Kommunikation sowie Partitionierung. Lückenlose Überwachung der Kommunikation ist geboten, um Cyberattacken frühzeitig zu erkennen. Domänenspezifische virtuelle Teilnetze (VLANs) minimieren im Fall eines Angriffs die Eindringtiefe. Beides ist in hybriden Bordnetzen machbar, erfordern allerdings für die CAN- und die Ethernet-Welt verschiedene methodische Ansätze.

### Effiziente Angriffserkennung für CAN

Zur Überwachung der CAN-Busse lässt sich ein Intrusion Detection System (IDS) in Gateways oder zentrale Steuergeräte integrieren. Anomalien im CAN-Datenverkehr erkennt es im Abgleich mit dem vom OEM spezifizierten „Normalverhalten". Die eingebettete Security-Komponente erkennt beispielsweise Anomalien bei

zyklischen Botschaften sowie missbräuchliche Diagnoseanforderungen, die es jeweils als potenzielle Angriffe klassifiziert und loggt bzw. meldet (Bild 1).

Die Leistungsfähigkeit des CAN-IDS (CycurIDS) hängt direkt von der Qualität seiner Konfiguration ab. Daher sollten effiziente initiale Regeln des OEM kontinuierlich durch neue Erkennungsmechanismen auf Basis von Analysen aktueller Angriffsvektoren ergänzt werden, um eine hohe Erkennungsrate bei möglichst wenigen Fehlalarmen zu erreichen. Die Umsetzung steht und fällt mit der Qualität des Werkzeugkastens, der bei der initialen Konfiguration und der kontinuierlichen Weiterentwicklung der Regelsätze zum Einsatz kommt. Als Ready-to-Use-Software ist das IDS (CycurIDS) als CAN-Angriffserkennung in hybriden Bordnetzen jederzeit einsatzbereit.

## Automotive Firewall im Ethernet Switch

Für die sichere, reibungslose Ethernet-Kommunikation in hybriden Bordnetzen hingegen ist eine Automotive Ethernet Firewall (CycurGATE) das Mittel der Wahl. Wird diese direkt im Ethernet Switch implementiert, kann sie den kompletten Packet Flow überwachen, ohne dass Interferenzen mit Steuergeräten oder dem Host Controller drohen. Durch ausbalanciertes Co-Design von Hard- und Software kann die Firewall die Hardwarebeschleunigung auf dem Switch optimal nutzen. Das Gros der Datenpakete wird so mit Wirespeed verarbeitet. Hauptaufgabe ist die Abwehr von Denial-of-Service Attacken. Doch indem die Firewall die Partitionierung in allen Netzwerkschichten aufrechterhält, unterstützt sie auch den sicheren Datenaustausch zwischen partitionierten Domänen. Hierfür filtert ein „Packet Filter" die ein- und ausgehenden Daten, die jeweils per „Stateful Packet Inspection" und vertiefter „Deep Packet Inspection" überprüft werden.

Die Automotive Ethernet Firewall (CycurGATE) schützt das Bordnetz also nicht nur vor unbefugtem Zugriff und Manipulation, sondern dient obendrein zur Steuerung der On-Bordkommunikation (Bild 2). Sie deckt den Ethernet/IP Stack inklusive der gängigen Automotive Protokolle (z. B. SOME/IP) vollständig ab und überwacht die Zugänge zu Netzen und VLANs. Gefiltert wird die Kommunikation anhand von jederzeit aktualisierbaren White- oder Blacklists, was die schnelle, wirksame Reaktion auf neue Angriffsmuster gewährleistet.

```
…
0.010000 1  100  Rx  d 8 8A FF FF 0C 42 5F FD 97
0.011000 1  110  Rx  d 8 03 3E 3E E2 10 FF 4A 3F
0.012000 1  120  Rx  d 8 03 F7 30 27 C7 7E D9 9C
0.020000 1  100  Rx  d 8 11 F4 00 3E E2 60 6C B9
0.021000 1  110  Rx  d 8 1F AA 00 00 00 00 C0 00
0.022000 1  120  Rx  d 8 02 AA 00 00 00 00 C0 00
0.031000 1  110  Rx  d 8 86 4A 2F 01 81 05 80 7F
0.031500 1  110  Rx  d 8 E5 2B 41 0C 00 00 00 00
0.032000 1  120  Rx  d 8 02 04 78 00 FF 00 00 30
0.041000 1  110  Rx  d 8 6E 7B FF FF 3F FF 1F 8B
0.042000 1  120  Rx  d 8 00 5A 00 00 0F 55 02 00
0.043000 1  7DF  Rx  d 8 02 10 03 00 00 00 00 00
0.044000 1  7E8  Rx  d 8 02 50 03 AA AA AA AA AA
0.051000 1  110  Rx  d 8 FE 4B 2F 01 81 07 80 7F
0.052000 1  120  Rx  d 8 68 05 78 00 FF 00 00 30
…
```

Timings
- Frequenzabweichung
- Nachrichteneinschleusung
- Timeouts

Diagnose
- Art des Services
- Service-Bedingungen

Bild 1: Das CAN-IDS erkennt Anomalien bei zyklischen Botschaften und den Missbrauch von Diagnoseanforderungen.

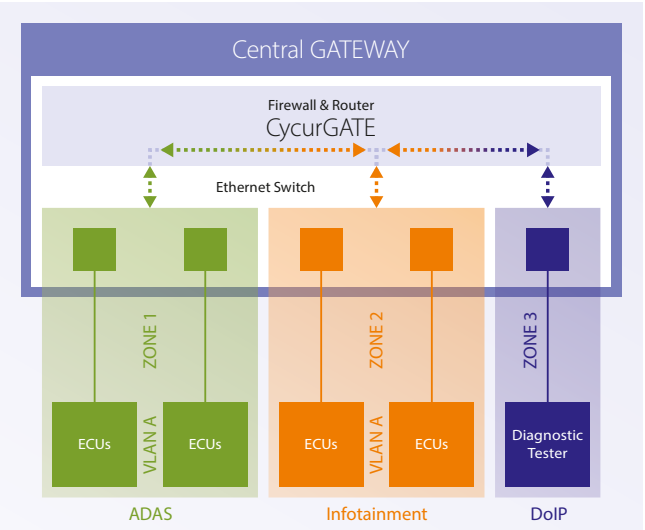



Bild 2: Automotive Ethernet Firewall übernimmt Gatekeeper- und Routerfunktionen.

## Intelligente Lastverteilung

Neben der Implementierung im zentralen Ethernet Switch ist es möglich, Host-basierte Firewalls direkt in Steuergeräte zu integrieren. Das setzt hoch performante Lösungen voraus. Die Firewall muss leistungsstark genug sein, um in Echtzeit zu prüfen und zu entscheiden, ob und wohin sie einzelne Datenpakete routet. Komplexe Angriffserkennungsmuster, etwa über die Frequenz der zustandsorientierten SOME/IP-Kommunikation, kann die Firewall nicht abdecken. Hier ist ein zusätzliches Ethernet-IDS geboten, das Muster von Anomalien anhand der Nachrichtenfrequenz, Sequenz, Nutzlastdaten und Services erkennt und als Angriffsversuche loggt bzw. meldet. Im Sinne optimaler Performance bedarf dieser Ansatz intelligenter Lastenverteilung zwischen Switch und Mikrocontroller. Firewalling und Intrusion Detection können teils im Switch und teils im Zielsteuergerät erfolgen.

Im Zusammenspiel können CAN-IDS, Automotive Ethernet Firewall und Ethernet-IDS hybride E/E-Architekturen zuverlässig und ohne merkliche Latenzen schützen. Eingebettet in ganzheitliche Security-Konzepte sind sie zentrale Bausteine der Risikoabwehr und der funktionalen Sicherheit im vernetzten und zunehmend automatisierten Fahrzeug der Zukunft. ■

## Autoren

**Dr. Jan Holle** ist Produktmanager Intrusion Detection Systems bei ESCRYPT. **M.Sc. Siddharth Shukla** ist Produktmanager Automotive Firewall bei ESCRYPT.


# AUTOSAR Security

## Adaptive-Plattform muss ganzheitlichen Fahrzeugschutz in den Blick nehmen

**Automatisierte Fahrfunktionen und zunehmende Vernetzung verlangen nach flexiblerer Software-Architektur – und einem hohen Grad an IT-Sicherheit. AUTOSAR trägt dem Rechnung. Mit der Adaptive Plattform und der Bereitstellung wichtiger Security-Komponenten.**

Noch erfüllt AUTOSAR Classic als Standard-Middleware für die meisten Fahrzeugplattformen die gängigen Anforderungen. Künftig jedoch werden Vehicle Computer als zentrale Instanzen die E/E-Architekturen prägen und das Fahrzeug wird zu einem softwaredominierten System. AUTOSAR Adaptive wird daher AUTOSAR Classic als neues zukunftsweisendes Regelwerk sukzessive ablösen – und dabei auch für die Automotive Security neue Standards setzen.

### Security-Bausteine in AUTOSAR

AUTOSAR beinhaltet bereits verschiedene IT-Sicherheitsanwendungen, etwa zur Absicherung der fahrzeuginternen Kommunikation oder zum Schutz vertraulicher Daten. Allerdings bieten Classic und Adaptive AUTOSAR derzeit aufgrund ihrer unterschiedlichen Architekturen teils gleiche, teils unterschiedliche Security-Anwendungen (Bild 1).

- **Crypto Stack:** Eruiert die implementierten kryptografischen Verfahren und Schlüsselspeicher und stellt den verschiedenen Applikationen über einheitliche Schnittstellen das nötige Schlüsselmaterial zur Verfügung. Die Applikationen greifen dann, unabhängig von ihren Krypto-Implementierungen, nur auf die bereitgestellten Schnittstellen zu und bleiben auf verschiedene ECUs portierbar. Zudem kann der AUTOSAR Crypto Stack parallel mehrere Krypto-Implementierungen unterstützen.
- **SecOC, TLS und IPsec:** SecOC sichert als AUTOSAR Classic-spezifisches Protokoll speziell die CAN-Kommunikation ab. SecOC gewährleistet Authentizität und Aktualität, jedoch keine Vertraulichkeit und erlaubt OEMs, Sicherheitsstufen granular anzupassen. TLS und IPsec dagegen werden mit Automotive Ethernet im Fahrzeug zunehmend bedeutsam. Beide Standards unterstützen authentische und vertrauliche Kommunikation; TLS ist auch für die externe Kommunikation geeignet.
- **Identity- & Access-Management:** Das AUTOSAR-Modul „Identity- und Access-Management“ sorgt dafür, dass nur autorisierte Anwendungen auf bestimmte Ressourcen zugreifen. Diese Zugriffsrechte können in AUTOSAR frei konfiguriert und jederzeit upgedatet werden.

- **Secure Diagnostics:** AUTOSAR unterstützt zum einen das Logging von IT-Sicherheitsereignissen in sicheren Speichern. Zum anderen wacht AUTOSAR über den autorisierten Zugriff auf diese Daten mittels der UDS-Dienste 0x27 (SecurityAccess) und 0x29 (Authentication). Der Diagnosetester beispielsweise erhält erst dann Zugriff auf die geloggten Security Incidents, wenn er zuvor eine Challenge-Response-Kommunikation durchgeführt oder sich per Zertifikat authentifiziert hat.

### Security-Engineering-Prozess

Entscheidend ist, die in AUTOSAR enthaltenen Security-Bausteine zur Anwendung zu bringen und entsprechend dem Security-Bedarf der Fahrzeugplattform individuell anzupassen. Das heißt, AUTOSAR muss durchgängig in den Security-Engineering-Prozess integriert werden. Drei Schritte sind dabei von ausschlaggebender Bedeutung: Risikoanalyse, Konfiguration und Testing. Für SecOC etwa würde sich das wie folgt darstellen (Bild 2):

- **Risikoanalyse:** Mittels Risikoanalyse aller Nachrichten werden diejenigen identifiziert, die per SecOC geschützt werden müssen. Sind unterschiedliche Security-Profile hinterlegt, wird die Nachricht dem richtigen Profil zugeordnet.
- **Konfiguration:** Im nächsten Schritt werden SecOC und Crypto Stack bei allen am Datenaustausch beteiligten ECUs gemäß der Risikobewertung und Security-Profile konfiguriert. Hier ist Sorgfalt geboten: Die Fehlkonfiguration in einer einzigen ECU kann zur Folge haben, dass gesicherte Nachrichten nicht verifiziert und damit verworfen werden.
- **Testing:** Aus Security-Perspektive müssen vor Freigabe einer ECU für die Serienproduktion mehrere Tests durchgeführt werden: Code Review der Security-kritischen Komponenten (z. B. SecOC-Modul, Crypto Stack), Penetration Test der ECU, Funktionstest des SecOC-Moduls.

### Arbeitsauftrag an AUTOSAR Adaptive

Auf dem Weg hin zum vernetzten, automatisiertem Fahren steigt die Zahl Safety-relevanter Funktionen im Fahrzeug. Elaboriertere Security-Maßnahmen und ein hohes Security-Level der Fahrzeugplattformen werden damit wichtiger denn je. Auch etablieren OEMs künftig vermehrt neue, auf hoher Konnektivität basierende Geschäftsmodelle, die es abzusichern gilt. Für die weitere Entwicklung von AUTOSAR Adaptive besteht daher der klare Arbeitsauftrag, Security-Anwendungen viel stärker als bisher zu integrieren.

Richtschnur für AUTOSAR Adaptive muss dabei ein ganzheitlicher Automotive Security-Ansatz sein: Zusätzliche IT-Sicherheitskomponenten wie Hardware-Security-Module und die mögliche Implementierung von Intrusion-Detection-and-Prevention-Lösungen werden daher bei der Weiterentwicklung von AUTOSAR Adaptive Berücksichtigung finden müssen. ■

## AUTOSAR-Konfiguration gemäß Security-Anforderungen

**Beispiel: Authentisierte ECU-Kommunikation**

- ✔ Identifikation Security-relevanter Nachrichten
- ✔ Konfiguration der Nachrichten in SecOC
- ✔ Auswahl der Schlüssel und Algorithmen im Crypto Stack
- ✔ Abstimmung der Konfigurationen im gesamten Fahrzeug
- ✔ Code Review der Security-kritischen Komponenten
- ✔ Penetration Test der ECU
- ✔ Funktionstest des SecOC-Moduls

Bild 2: AUTOSAR-Konfiguration gemäß Security-Anforderungen am Beispiel SecOC.


### Autoren

**Dr. Alexandre Berthold ist** Teamleiter für Consulting und Engineering bei ESCRYPT. **Dr. Michael Peter Schneider** ist Project Manager AUTOSAR-Security bei ESCRYPT.


| | Crypto Stack | SecOC | TLS | IPSec | Secure Log/Diag | Identity & Access Mgmt |
|---|---|---|---|---|---|---|
| AUTOSAR Classic 4.4 | ✔ | ✔ | ✔ | ✖ | ✔ | ✖ |
| AUTOSAR Adaptive R19-03 | ✔ | ✖ | ✔ | ✔ | ✖ | ✔ |

Bild 1: Security-Anwendung in AUTOSAR Classic und Adaptive (Stand August 2019).

# Digitale Schutzimpfung für das Steuergerät

## IT-Security für das vernetzte Fahrzeug beginnt in der Steuergeräteproduktion

**Wie kann das für einen sicheren Datenaustausch notwendige kryptografische Schlüsselmaterial anforderungsgerecht in die ECUs eingebracht werden? Die Antwort liefert eine integrierte Lösung aus zentralem Key Management Backend und dezentralen Production Key Servern.**

Beim Schutz vor Cyberangriffen kommt den Steuergeräten im Fahrzeug im wahrsten Sinne des Wortes eine Schlüsselrolle zu: Erst kryptografische Schlüssel erlauben es den ECUs, sich zu authentifizieren und damit den Datenaustausch innerhalb des Bordnetzes, aber auch nach außen hin zu legitimieren. Die besondere Herausforderung dabei: Die Steuergeräte für die verschiedenen Fahrzeugplattformen müssen initial mit dem OEM-spezifischen Schlüsselmaterial und Zertifikaten versorgt werden – und das idealerweise bereits bei deren Produktion durch den ECU-Hersteller.

### Sichere Distribution des OEM-Schlüsselmaterials

Die probate Lösung liegt in einer Verbindung aus klassischem Key-Management-System (KMS) als zentralem Backend und mit dem KMS kommunizierenden, dezentral installierten Production Key Servern (PKS) in den Produktionsstätten. Vorteil für den OEM: Die Bestückung seiner spezifischen elektronischen Steuergeräte mit dem eigenen Schlüsselmaterial lässt sich vollständig in die bestehende Produktionsinfrastruktur des ECU-Zulieferers integrieren. Dabei werden dabei die Datenpakete mit dem vom jeweiligen Autohersteller bereitgestellten Schlüsselmaterial in das KMS eingespeist.

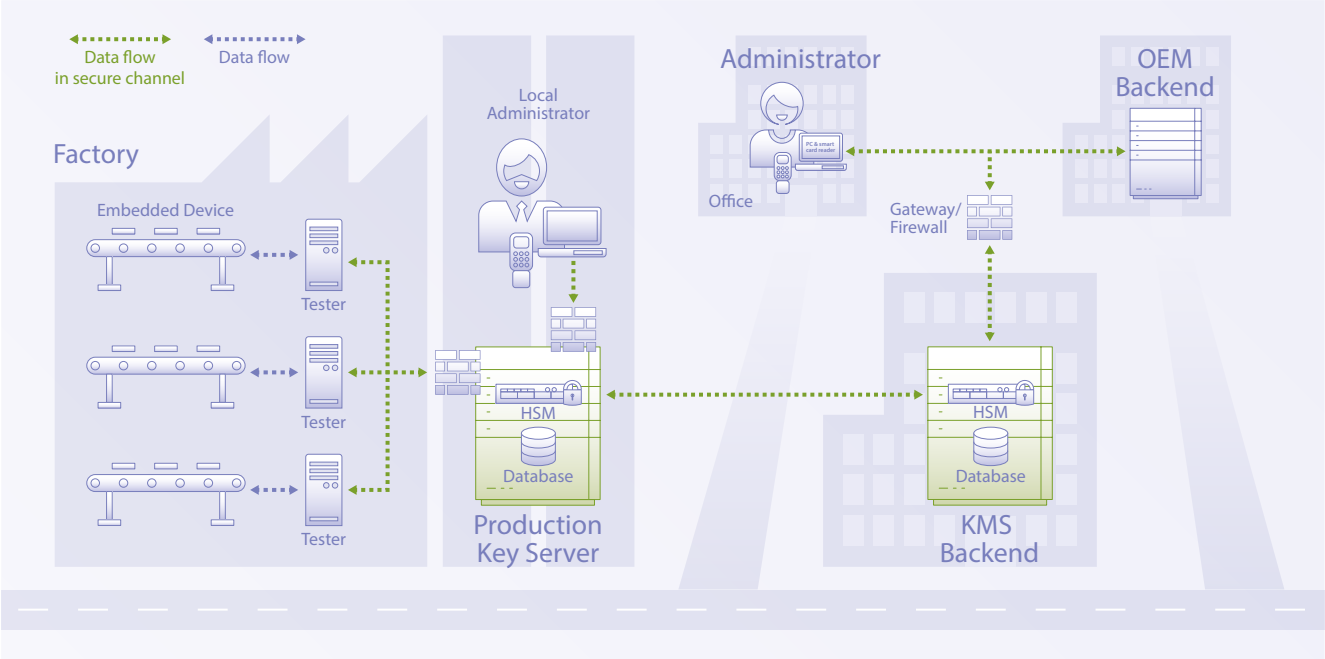



Bild 1: Integrierte Key Distribution und Injection mit Key Management Solution und Production Key Server

Das Schlüsselmaterial wird zentral gespeichert, per sicherer Datenübertragung bedarfsgerecht an die Produktionsstandorte verteilt und dort auf Production Key Servern bevorratet (Bild 1).

### Einbringen der Schlüssel per End-of-Line-Tester

Das Einbringen des Schlüsselmaterials in die Steuergeräte erfolgt vor Ort in der Fertigung durch angebundene End-of-Line-Tester. Diese rufen die einzelnen Schlüsselpakete dann beim Production Key Server im Werk ab und „injizieren" sie – einer „digitalen Schutzimpfung" gleich – während der Produktion in die einzelnen Steuergeräte. Gleichzeitig protokolliert der PKS, welche kryptografischen Schlüssel in welche ECU eingebracht wurden. Auf Wunsch werden abschließend so genannte Verification Files aus der Fertigung vom PKS über das zentrale KMS-Backend zum OEM zurückgespielt. Der Autohersteller hat so die Gewissheit, dass die Fahrzeugsteuergeräte mit seinem Schlüsselmaterial korrekt bedatet sind.

### Sichere Bevorratung ohne ständige Online-Anbindung

Besonderer Vorteil der Lösung ist die Symbiose aus hoher Sicherheit und Verfügbarkeit. Denn die Production Key Server sind sowohl durch ein robustes und leistungsfähiges Hardware-Sicherheitsmodul (HSM) als auch durch eigene Sicherheitssoftware vor unerlaubtem Zugriff geschützt. Zudem treten die PKS nur von Zeit zu Zeit in Kontakt mit dem Backend, um den Datenbestand zu synchronisieren, etwaige Updates vorzunehmen und ausreichende Puffer mit kryptografischen Daten anzulegen. Das heißt, sie sind nicht auf eine permanent stabile Internetanbindung angewiesen und so vor potenziellen Onlineattacken weitgehend gefeit.

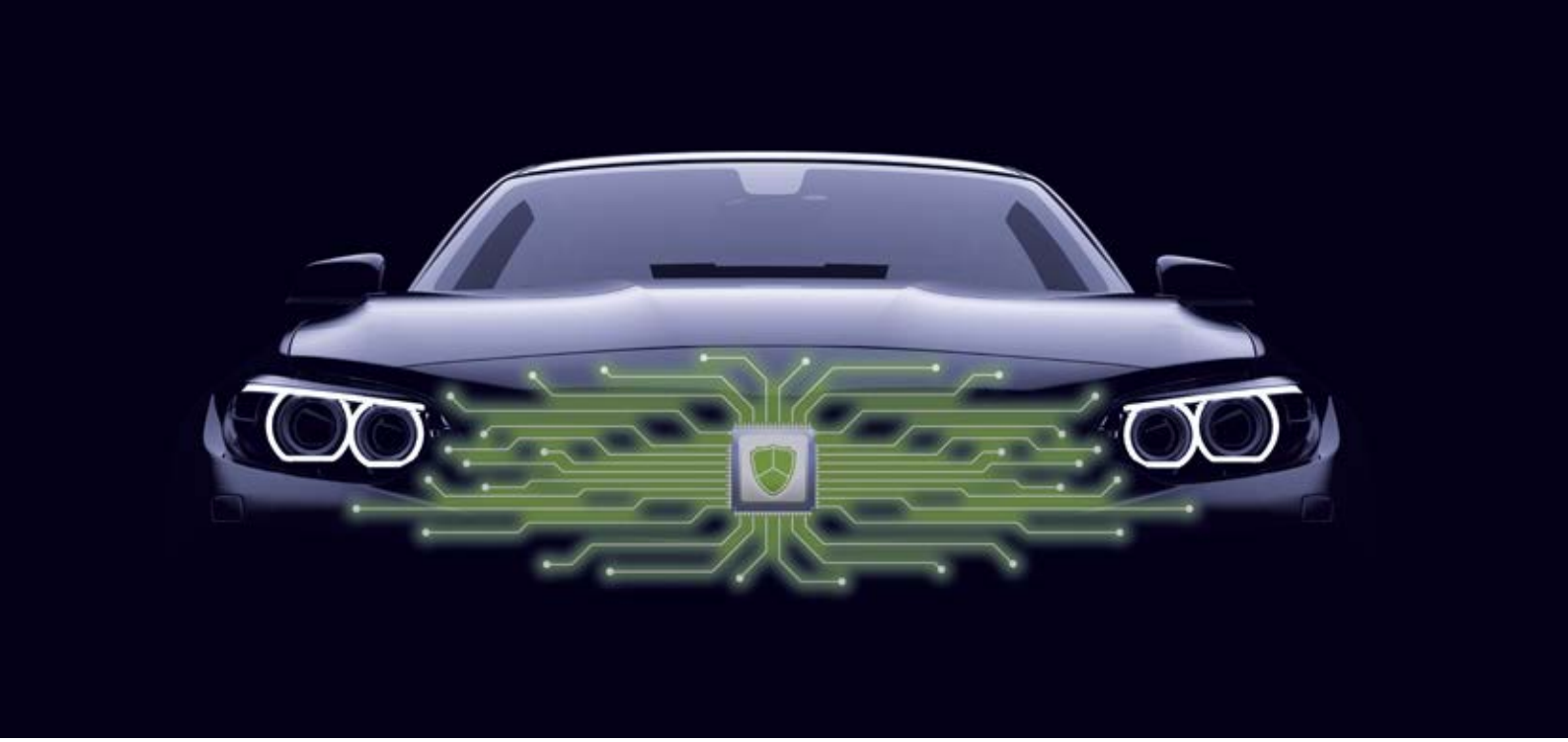
Wie oft die Kontaktaufnahme zum KMS-Backend erfolgen soll, können die Nutzer bedarfsgerecht bestimmen. Sinkt der Bestand unter ein vorgegebenes Mindestkontingent, werden vom Server automatisch neue Schlüssel angefordert. Auf diese Weise ist gewährleistet, dass stets genügend Schlüsselmaterial für die Bestückung der Fahrzeugsteuergeräte in der Fertigung vorrätig ist. Ein potenziell kostspieliger Produktionsausfall durch eine unterbrochene Netzwerkverbindung ist ausgeschlossen. Der Production Key Server bleibt stets einsatzbereit.

### Weltweit in der ECU-Produktion im Einsatz

Eine sichere und präzise Bedatung von Fahrzeugsteuergeräten mit kryptografischen Schlüsseln bildet das Fundament für nahezu alle weiteren IT-Sicherheitsfunktionen im Fahrzeug. Die integrierte KMS-PKS-Gesamtlösung ermöglicht es, den komplexen Auslieferungsmechanismus von kryptografischem Material des OEM über ein sicheres Key-Management, die sichere Bevorratung und Injektion des Schlüsselmaterials in die ECUs bis hin zur Protokollierung und Verifikation zu meistern. Aus gutem Grund ist dieses Verfahren heute weltweit bei der Steuergeräteproduktion für verschiedene Automobilhersteller im Einsatz. ■


### Autoren

**Christian Wecker** ist Product Manager PKS bei ESCRYPT.
**Michael Lueke** ist als Senior Program Manager KMS bei ESCRYPT.



# Leistungsschub für Hardware-Security-Module

## Neue Service-orientierte 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 (HSM) der neuen Generation werden zum zentralen Baustein. Denn sie vereinen Multi-App-Fähigkeit mit Echtzeit-Kommunikation.**

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 Softwareapplikationen 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 Softwareapplikationen 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.

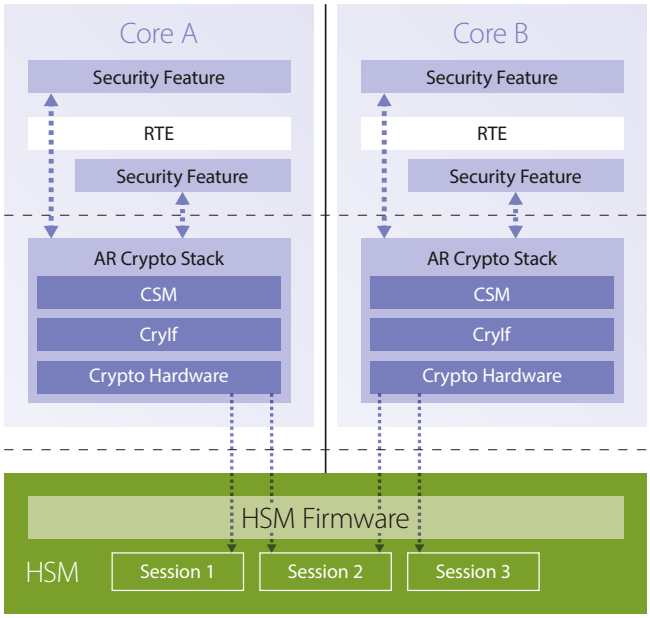



Bild 1: Anfragen mehrerer Host-Cores werden von der HSM-Firmware in parallelen Sessions verarbeitet.

Für eine rundum abgesicherte Onboard-Kommunikation (SecOC) sind u. a. 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 Virtual Machines partitionierte Vehicle Computer Softwareanwendungen 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 On-Board Communication, Runtime Manipulation Detection, sicheres Booten, Flashen, Loggen oder Debuggen. Damit sind HSM deutlich leistungsstärker als rein softwaregestützte IT-Sicherheitslösungen.

Werden Softwareanwendungen 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 HSM stoßen hier an Grenzen; softwaregestützte Security-Lösungen erst recht. Doch eine neue Generation von Hardware-Security-Modulen mit Real-time-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 neuer 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, so dass 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-Modul. 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).

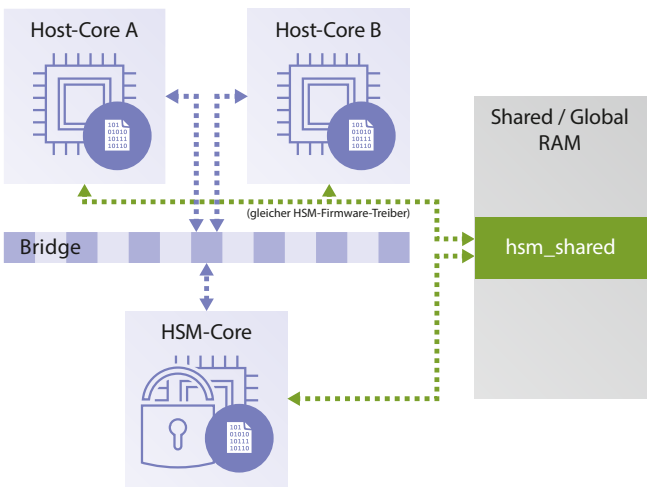



Bild 2: Multi-Core- / Multi-Application-Support – Job Requests werden per Bridgeregister und Shared RAM abgearbeitet.

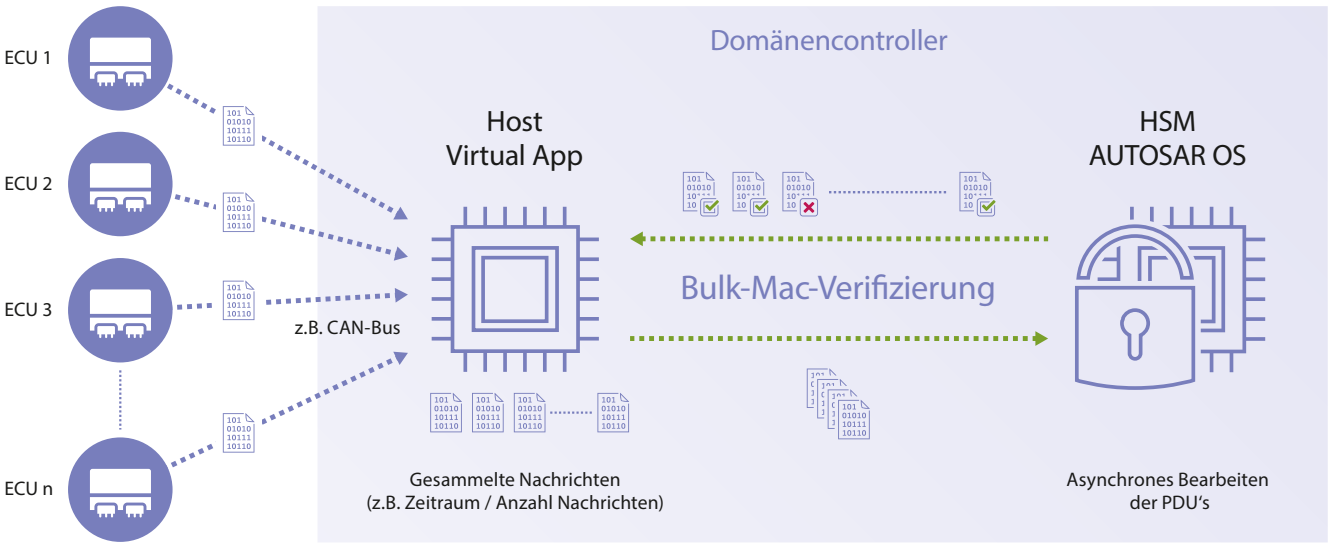



Bild 3: Das Bulk-Mac-Interface sorgt für sichere Echtzeitkommunikation.

### 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 HSM eine Lösung, obwohl ihr Leistungsvermögen nicht unbegrenzt ist. Limits 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-Hardwareeinheit 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 Echtzeit-Kommunikation 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 Softwareanwendungen mit hoher Datenlast und unter Echtzeitanforderung abzusichern.

Mit Blick auf die zunehmende Konnektivität und den Trend zum automatisierten Fahren setzen OEMs vermehrt 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 Tier1s 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 Cyber Security Solutions bei ESCRYPT.

Planungsansicht Mark 51°7, Bochum. © skt umbaukultur – Partnerschaft von Architekten mbB – Bonn

# ESCRYPT plant neues Headquarter

**Auf dem ehemaligen Opel-Werksgelände in Bochum wird bis Anfang 2022 die neue ESCRYPT-Unternehmenszentrale entstehen. Ab Sommer wächst dort entlang modernster baulicher und energetischer Standards ein neues Headquarter in die Höhe, das zukünftig bis zu 500 Mitarbeiterinnen und Mitarbeitern ein attraktives Arbeitsumfeld bietet.**

„Mit dem neuen Standort stärken wir bewusst die Nähe zur pulsierenden Hochschul- und Forschungslandschaft der Region", so Dr. Uwe Müller, verantwortlicher Geschäftsbereichsleiter für ESCRYPT innerhalb der Bosch-Gruppe. Zugleich steht der Neubau auf dem früheren Opel-Areal sinnbildlich für den Wandel der Automobilbranche fort vom reinen Fahrzeugbau hin zur digital vernetzten und automatisierten Mobilität. ■

Dr. Uwe Müller,
Leiter Geschäftsbereich Cybersecurity Solutions,
ESCRYPT (Bosch Group)

*„Mit dem neuen Standort stärken wir bewusst die Nähe zur pulsierenden Hochschul- und Forschungslandschaft der Region."*


**Das Gute wacht immer und überall**

ESCRYPT hat Automotive Security neu vermessen. Mit ganzheitlichen IT-Sicherheitslösungen schützen wir Ihre Fahrzeugflotte immer und überall – in der Produktion, auf der Straße und im Backend.

**www.escrypt.com**

escrypt

SECURITY. TRUST. SUCCESS.