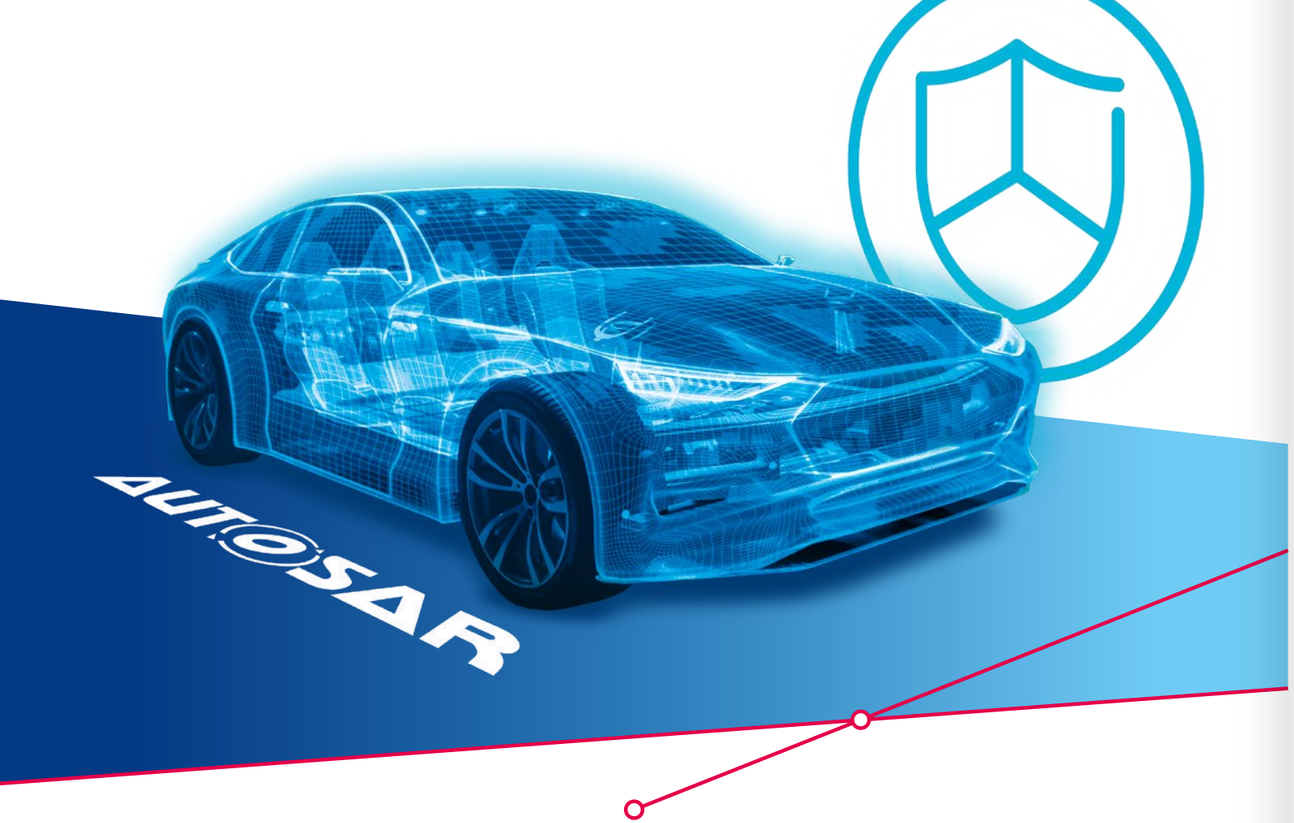


Cybersecurity inklusive

Sicherheit für AUTOSAR-Adaptive-Architekturen

Der Weg zum intelligent vernetzten Fahrzeug führt über AUTOSAR Adaptive. Für verlässlichen Schutz gegen Cyberangriffe hält dieser Standard Security-Funktionen bereit, die sich per Plattformsoftware-Framework schon heute in die E/E-Architekturen von morgen integrieren lassen.

E/E-Architekturen mit signalbasierter Vernetzung und funktional aufgeteilten Steuergeräten (ECUs) stoßen in vernetzten und hochautomatisierten Fahrzeugen an ihre Grenzen. Die Forderung nach Autonomie und Konnektivität führt dazu, dass zentrale, hochperformante Vehicle Computer (VCs) und Domänencontroller (DCUs) die strategischen Entscheidungen zentral treffen. Sensor- und Aktor-Steuergeräte führen dann nur noch die Befehle aus.

Die AUTOSAR-Adaptive-Plattform setzt den Rahmen für diese neuen E/E-Architekturen. Sie erlaubt es, Anwendungssoftware dynamisch anzupassen und schafft mit der Schnittstelle „AUTOSAR Runtime for Adaptive Applications" (ARA) die Verbindung zum POSIX-basierten Betriebssystem, wie zum Beispiel Linux (Bild 1). Für den sicheren Betrieb von Software unterschiedlicher Anbieter und verschiedener ASIL-Kategorien auf den VCs ist deren vorkonfigurierte Partitionierung per Hypervisor vorgesehen.

Cybersecurity-Management

Intelligent vernetzte Fahrzeuge sind nicht mit Einzelmaßnahmen abzusichern. Ganzheitliche Konzepte auf Basis von Risikoanalysen der gesamten Fahrzeugarchitektur sind gefragt. Diese gilt es, auf die Security-Anforderungen der einzelnen Komponenten, ECUs sowie deren logische Partitionen herunterzubrechen. Um dies umzusetzen, ist in AUTOSAR Adaptive ein Basis-Set an Security-Funktionen integriert, mit dem Entwickler den quantitativ und qualitativ wachsenden Schutzbedarf der vernetzten automatisierten Fahrzeugsysteme adressieren können. Da die zentralisierte, softwarebasierte E/E-Architektur auch die Datenlasten unter Echtzeitbedingungen in die Höhe treibt, müssen Security-Maßnahmen entsprechend performant ausgelegt werden. Dafür sind in AUTOSAR Adaptive die nachfolgend vorgestellten Security-Funktionen integriert (Bild 2 nächste Seite).

Kryptografie als „Schlüssel-Komponente"

Viele Security-Anwendungsfälle setzen auf kryptografische Primitive, um zum Beispiel vertrauliche Daten zu verschlüsseln oder die Signatur von Software-Updates zu verifizieren. Die dafür nötigen kryptografischen Schlüssel und Zertifikate müssen sicher gespeichert, von einer autorisierten Anwendung verwaltet und zuweilen über mehrere Steuergeräte synchronisiert werden. In AUTOSAR Adaptive werden diese Primitive durch den „Cryptography Functional Cluster" (auch Crypto API genannt) bereitgestellt. Er bietet eine Abstraktion der bereitgestellten Schnittstellen und erhöht somit die übergreifende Software-Portabilität.

Für sicheren Datenaustausch setzt AUTOSAR Adaptive auf moderne Standards, darunter TCP/IP-Kommunikation via Ethernet. Über die in der IT-Welt etablierten Protokolle TLS und IPSec lassen sich sichere Kanäle für die Kommunikation im Fahrzeug und mit externen Instanzen konstituieren, die nicht manipuliert oder abgehört werden können.

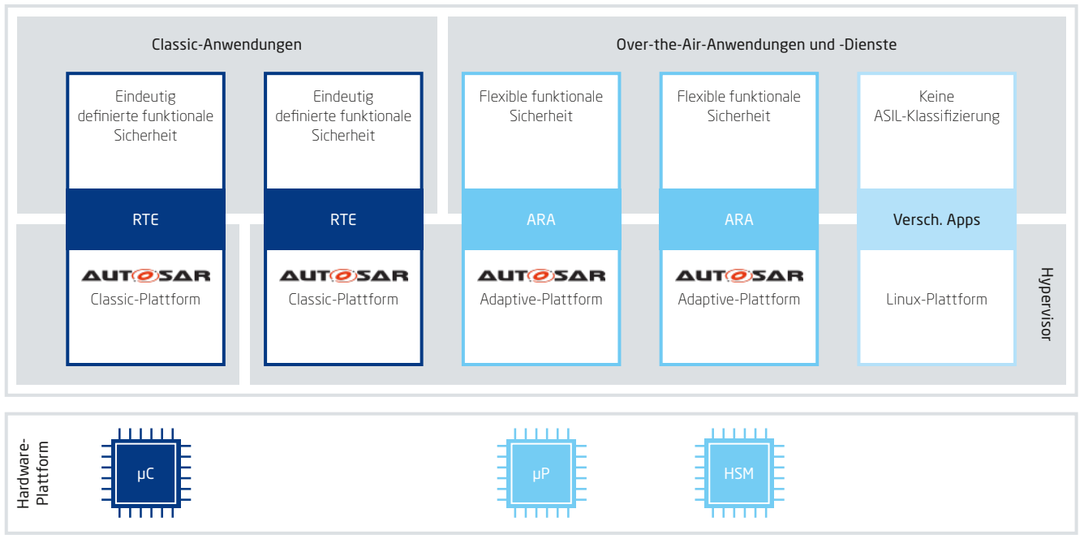
AUTOSAR Adaptive regelt den Zugriff auf Systemressourcen, wie persistente Speicher, Kommunikationskanäle, kryptografische Schlüssel etc. Mit dem AUTOSAR-Modul Identity- und Access-Management steht ein Torwächter bereit, der nur explizit autorisierte Anwendungen auf die jeweilige Ressource zugreifen lässt. Die Zugriffsrechte lassen sich bedarfsgerecht konfigurieren und jederzeit aktualisieren.

Secure Update und Trusted Platform

Die Secure-Update-Funktion in AUTOSAR Adaptive hilft dabei, (zum Beispiel mithilfe von Intrusion Detection System, IDS) erkannte Schwachstellen zu beheben. Dazu empfängt und verarbeitet sie Security-Updates für einzelne Applikationen oder sogar für die gesamte Plattform. Die einzelnen Update-Blobs werden dabei vom Backend signiert, sodass nur Updates aus vertrauenswürdiger Quelle ausgeführt werden.

Neben den Updates brauchen auch die Anwendungen auf ECUs und VCs eine regelmäßige Überprüfung. Dazu dient Secure Boot beziehungsweise die Trusted-Platform-Funktion in AUTOSAR Adaptive. Sie verifiziert als Vertrauensanker (Trust Anchor) alle Anwendungen und die Plattform als solche. Indem so eine Vertrauenskette vom Boot über die Plattform bis zur Anwendung aufrechterhalten wird, ist sichergestellt, dass nur vertrauenswürdige Software ausgeführt wird.

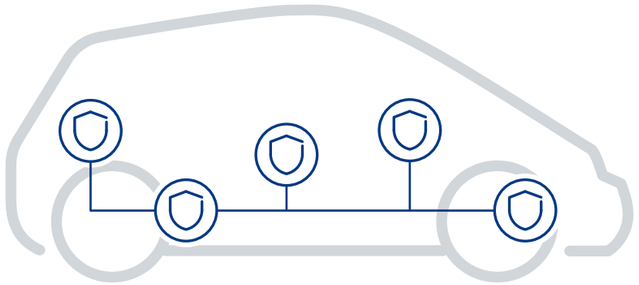
Bild 1: Während AUTOSAR-Classic-Systeme mit harten Echtzeitanforderungen unterstützt, profiliert sich AUTOSAR Adaptive als Standard für dynamische Anwendungen.



RTE = Runtime Environment
µC = Mikrocontroller

ARA = AUTOSAR Runtime for Adaptive Applications
µP = Mikroprozessor

API = Programmierschnittstelle
HSM = Hardware-Security-Modul



Security-Komponenten in AUTOSAR Adaptive

- **Krypto-Stack** zur Verwaltung von Schlüsselmaterial und Zugriff auf Krypto-Primitive
- **Sichere Kommunikation** über die etablierten Protokolle TLS und IPSec
- **Zugriffsschutz** für sensible Ressourcen (z. B. Schlüssel) über das Modul Identity- und Access-Management
- **Sichere Updates** von einzelnen Applikationen bis hin zur kompletten Plattform
- **Authentische Software** durch Fortführung der Secure-Boot-Vertrauenskette im Rahmen der „Trusted Platform"

Bild 2: Zentrale Security-Komponenten in AUTOSAR Adaptive.

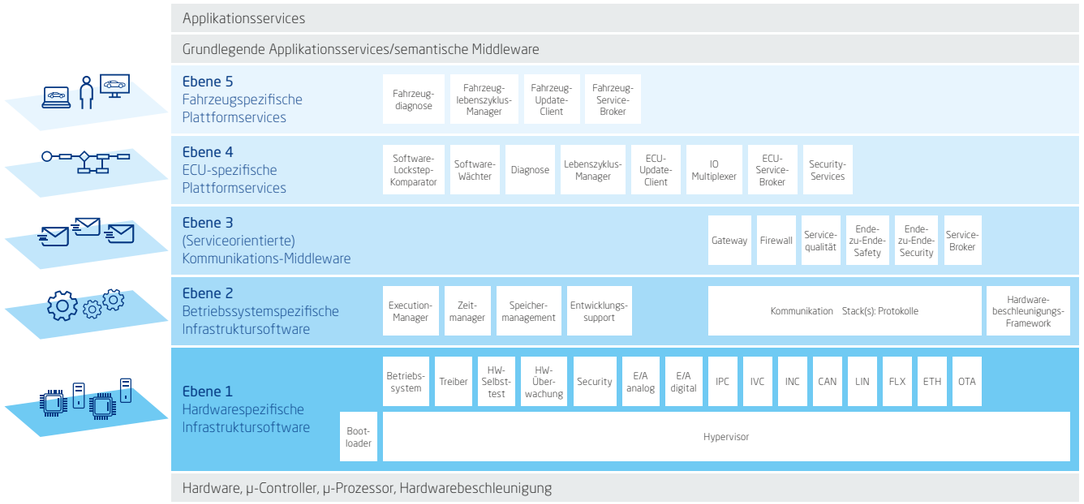
RTA-VRTE: Plattformsoftware-Framework für AUTOSAR Adaptive

Für künftige Anwender von AUTOSAR Adaptive ist es von existenzieller Bedeutung, sich schon heute mit der neuen Architektur vertraut zu machen. Das Plattformsoftware-Framework RTA-VRTE (Vehicle Runtime Environment) bietet dafür die ideale Basis; sei es zur Integration und Implementierung von Security-Funktionen oder für alle weiteren AUTOSAR-Adaptive-konformen Prozesse.

RTA-VRTE enthält alle wichtigen Middleware-Elemente für mikroprozessorgestützte Fahrzeugrechner. Das Plattformsoftware-Framework erlaubt es, die Funktion virtueller ECUs auf herkömmlichen Desktop-PCs zu simulieren und per Ethernet zu vernetzen. RTA-VRTE erzeugt dazu eine virtuelle Maschine, die eine aus vier Ebenen aufgebaute Basissoftware-Architektur enthält. Auf einer fünften Ebene sind dann die fahrzeugspezifischen Plattformservices aufgesetzt (Bild 3).

Die Ebenen 1 und 2 beheimaten Infrastruktursoftware der eingesetzten Hardware (zum Beispiel Gerätetreiber) und ein POSIX-konformes Betriebssystem. Zudem birgt Ebene 2 Elemente, die sich aus den AUTOSAR-Adaptive-Spezifikationen ableiten – zuvorderst das Execution Management. Dieses verwaltet die dynamisch zugewiesenen Anwendungen, stellt sicher, dass sie korrekt starten und enden und es wacht über das Einhalten der zugewiesenen Ressourcen- und Ausführungslimits. Damit ist das Execution Management in puncto IT-Sicherheit eine Schlüsselfunktion: Es stellt die Trusted Platform bereit und prüft die Integrität und Authentizität der Adaptive-Anwendungen. So werden etwaige Manipulationen oder Beschädigungen schon vor dem Start erkannt.

Bild 3: Das Fünf-Ebenen-Modell der RTA-VRTE unterstützt die wichtigen Softwarefunktionen und -anforderungen für Vehicle Computer.



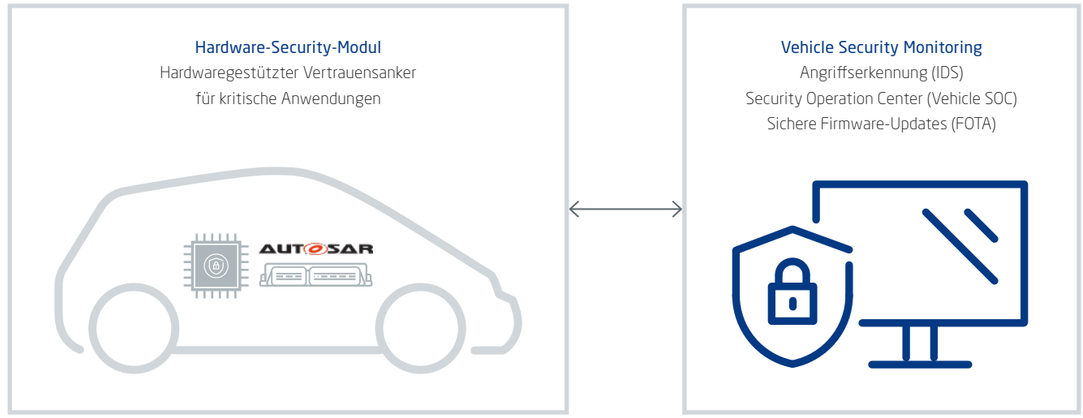


Bild 4: Ganzheitliche Automotive-Cybersecurity mit Hardware-Security-Modul als Vertrauensanker im Mikrocontroller und Vehicle Security Monitoring über den gesamten Fahrzeuglebenszyklus hinweg.

Daneben stellt eine Kommunikations-Middleware auf Ebene 3 sicher, dass die dynamischen, flexiblen Adaptive-Anwendungen und die anderen Software-Anwendungen im System interagieren können. Als Kernkomponente des RTA-VRTE steuert und regelt das Kommunikationsmanagement die Interaktion zwischen den Ebenen und garantiert den reibungslosen Betrieb der gekapselten Software inklusive der steuergeräte- und fahrzeugabhängigen Plattformservices auf den Ebenen 4 und 5. Im Sinne einer sicheren End-to-End-Kommunikation zwischen den Services authentifizierter Anwendungen hat diese Funktion ebenfalls hohe Relevanz für die Cybersecurity.

Das RTA-VRTE-Kommunikationsmanagement samt steuergerätespezifischen Diensten auf Ebene 4 bietet Anwendungsentwicklern ein vielseitiges Rahmenwerk für Automotive-Anwendungen. Für die Security ist auf dieser Ebene ein Update and Configuration Manager (UCM) verfügbar, der authentifizierte Updates einzelner Anwendungen unterstützt und über die gesamte Plattform hinweg koordiniert. Auf Ebene 5 des RTA-VRTE lassen sich im Sinne von AUTOSAR++ Funktionen für das Gesamtfahrzeug oder sogar für die gesamte Flotte integrieren – bis hin zu robusten Over-the-Air-Updates des RTA-VRTE-AUTOSAR-Adaptive-Anwendungssets.

Ausblick: Ganzheitliche Security über AUTOSAR Adaptive hinaus

Seit 2020 wird RTA-VRTE weltweit in Projekten eingesetzt, die AUTOSAR-Adaptive-Fahrzeugplattformen für die Serienproduktion zum Ziel haben. Daneben bieten ETAS und ESCRYPT ein Early Access Program (EAP) an, mit dem OEMs und Zulieferer die Entwicklungsmethodik hybrider E/E-Architekturen der nächsten Generation erarbeiten – und dabei die bereits in AUTOSAR Adaptive verfügbaren Security-Komponenten implementieren.

Über diese Security-Bausteine hinaus setzt ein wirklich umfassender Schutz vernetzter, automatisierter Fahrzeuge ganzheitliche Cybersecurity-Konzepte voraus. Das beginnt bei Hardware-Security-Modulen (HSMs) als Vertrauensanker, um kryptografisches Schlüsselmaterial im VC-Mikrocontroller oder in ECUs physikalisch zu kapseln. Es reicht bis zu einem flottenweiten Schutz des Fahrzeugs über dessen gesamten Lebenszyklus hinweg, mitsamt einer im Fahrzeug eingebetteten Angriffserkennung, einem Vehicle Security Operation Center (VSOC) im Backend und Security-Updates via Firmware-Over-the-Air (FOTA), (Bild 4).

Das Plattformsoftware-Framework RTA-VRTE versetzt Entwickler in die Lage, AUTOSAR-Adaptive-basierte E/E-Architekturen schon heute virtuell zum Leben zu erwecken.
Damit erweitert es die Basis für einen ganzheitlichen Schutz vor Cyberangriffen, der sich im Fahrzeug der Zukunft vom Mikrocontroller über das fahrzeuginterne Netzwerk bis zum lebenslangen, flottenweiten Monitoring erstrecken wird.

Autoren

Dr. Michael Peter Schneider ist Project Manager AUTOSAR Security bei der ESCRYPT GmbH. **Dr. Stuart Mitchell** ist RTA-VRTE Senior Product Manager bei der ETAS GmbH.