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 in vielen Bereichen 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- und 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 (zum Beispiel SecOC-Modul, Crypto Stack), Penetration-Test der ECU und Funktionstest des SecOC-Moduls.

Arbeitsauftrag an AUTOSAR Adaptive

Auf dem Weg hin zum vernetzten, automatisierten 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

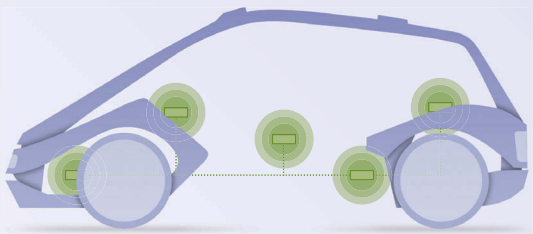

Bild 2: AUTOSAR-Konfiguration gemäß Security-Anforderungen am Beispiel SecOC.

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).