Neue E/E-Architekturen

Damit das Joint Venture nicht zum Cyberrisiko wird

Mit Hochgeschwindigkeit bewegen sich die Autohersteller in Richtung SDV. Partnerschaften mit anderen OEMs versprechen hier mehr Entwicklungspower und besseren Zugang zu regionalen Märkten. Doch wie lässt sich angesichts unterschiedlicher Technologien und Prozesse der Partner der nötige Cyberschutz der Fahrzeuge gewährleisten?

Wie lassen sich Cybersecurity, SecOC, OTA und IDS in SDV-Joint Ventures über unterschiedliche E/E-Architekturen hinweg harmonisieren?

Bild: ETAS

Volkswagen und Rivian, Daimler Truck und Volvo – in der Automobilindustrie setzt sich die Erkenntnis durch, dass man gemeinsam stärker ist. Die Entwicklung neuer Fahrzeugplattformen für das Software-definierte Fahrzeug (Software-defined vehicle SDV) setzt die OEMs unter Zeit- und Kostendruck. Lasten zu verteilen und Kompetenzen zu vereinen, ist da ein logischer Schritt.

Herausforderung für die Automotive Security

Für die Cybersicherheit der Fahrzeuge bringen solche Joint Ventures jedoch auch erhebliche Herausforderungen mit sich. Stellt bereits das SDV mit seiner Entkopplung von Hard- und Software, seinem erweiterten Ökosystem und seiner hohen Konnektivität ohnehin schon neue hohe Cybersecurity-Anforderungen, so fügt eine aus Komponenten unterschiedlicher Partner zusammengefügte Fahrzeugarchitektur der Komplexität nochmals eine neue Dimension hinzu. Im Wesentlichen lassen sich drei zentrale Problemfelder identifizieren:

- Harmonisierung der Security-Konzepte: Die Partner bringen in aller Regel über Jahre gewachsene Cybersecurity-Prozesse, -Technologien und -Softwarelösungen mit. Diese unterschiedlichen „Security Postures“ gilt es, zu einem einheitlichen, robusten Ganzen zusammenzuführen.
- Balance zwischen Security und Effizienz: Die Cybersicherheit darf die erhofften Vorteile der Partnerschaft nicht zunichtemachen. Security-Maßnahmen müssen von Beginn an so integriert werden, dass sie die Agilität nicht ausbremsen.
- Mögliche neue Angriffsflächen: Gemeinsame Architekturen schaffen neue technische Herausforderungen. Werden vormals getrennte Systeme verschiedener Partner integriert, entstehen zwangsläufig neue Schnittstellen, die es abzusichern gilt. Gefragt ist demnach ein ganzheitlicher Ansatz, der die Automotive Cybersecurity sowohl auf organisatorischer als auch auf technischer Ebene durchgängig und nachhaltig gewährleistet (Bild 1).

Organisatorische Weichenstellungen

Auf organisatorischer Ebene gilt es, von Beginn an klare Strukturen und Verantwortlichkeiten zu schaffen. Anstatt Cybersicherheit als nachgelagertes Thema zu behandeln, muss sie in der Partnerschafts-Governance fest verankert werden, idealerweise durch ein gemeinsames Gremium aus hochrangigen Security-Experten beider Partner. Dieses Komitee benötigt klare Entscheidungsbefugnisse für Cybersecurity-Standards, -Technologien und -Prozesse.

Ein zentraler Aspekt ist die Definition klarer Schnittstellen, die beispielsweise in einem „Cybersecurity Interface Agreement“ (CIA) nach ISO/SAE 21434 festgehalten werden können. Essenziell ist es auch, die Kooperation vom Ende her zu denken. Fahrzeuglebenszyklen von 15 Jahren und mehr überdauern viele Unternehmenspartnerschaften. Daher müssen die Verpflichtungen für die Zeit nach Produktionsstart (Post-SOP) – wie das kontinuierliche Schwachstellen-Monitoring, Incident Response und die Bereitstellung von Security-Updates – vertraglich unmissverständlich geregelt sein. Nur

so kann die Cybersicherheit des Fahrzeugs über den gesamten Lebenszyklus sichergestellt werden, selbst wenn das Joint Venture längst aufgelöst ist.

Harmonisierung vernetzter Security Controls

In partnerschaftlich entwickelten neuen E/E-Architekturen ist die Harmonisierung der Security Controls im Wesentlichen abhängig von Art und Grad ihrer Vernetzung. Rein lokale Schutzmechanismen, die autark innerhalb einzelner Fahrzeugsteuergeräte (Electronic Control Units ECUs) agieren, weisen in der Regel keinen oder nur geringen Harmonisierungsbedarf auf. Differenzierter zu betrachten sind Security Controls, die nicht fahrzeugintern, sondern lediglich mit einer externen Instanz (z.B. einem Backend) kommunizieren; bestes Beispiel ist hier Secure Update. Hier kann es je nach angestrebtem Zusammenarbeitsmodell sinnvoll sein, die Controls zu harmonisieren oder getrennte Backends beizubehalten.

Ganz anders bei Security Controls, die eine Kommunikation verschiedener Komponenten im Bordnetz erfordern. Hier ist die Harmonisierung der Security-Mechanismen Grundvoraussetzung dafür, dass sie funktionieren. Das gilt insbesondere auch für Schutzmechanismen, die auf Input aus anderen Security Controls und anderen Fahrzeugkomponenten angewiesen sind. In die Kategorie vernetzter Security Controls fallen typischerweise die sichere Kommunikation innerhalb des Fahrzeugs (inkl. Secure Onboard Communication SecOC, TLS, MACSec), Secure Updates, das Angriffserkennungssystem (Intrusion Detection System IDS) oder auch das Schlüsselmanagementsystem (Key Management System KMS).

Sichere Bordnetz-Kommunikation

Die Absicherung der Kommunikation zwischen den ECUs ist das Rückgrat der Automotive Cybersecurity. In klassischen Netzen (z. B. CAN, Flexray) sowie für signalbasierte Kommunikation über Ethernet bürgt AUTOSAR mit seiner Secure Onboard Communication (SecOC) auch weiterhin in ausreichendem Maße für Authentizität und Aktualität der übertragenen Daten. Der Standard allein ist jedoch keine Plug-and-Play-Lösung. Er lässt wichtige Implementierungsdetails offen, die in einer Partnerschaft zwingend harmonisiert werden müssen, so etwa

- der Freshness-Wert, der zwischen sendenden und empfangenden ECUs aufeinander abgestimmt sein muss, um Replay-Angriffe zu verhindern.
- das Schlüsselmanagement, das auf einheitliche Weise die für SecOC benötigten symmetrischen Schlüssel in die Steuergeräte einspeisen und den einzelnen Nachrichten zuordnen muss (siehe unten).
- die Parametrisierung des SecOC-Protokolls, um Interoperabilität zu gewährleisten.

Je nach Netzwerk-Topologie muss diese Harmonisierung nicht die gesamte Fahrzeugarchitektur umfassen. In einer zonale E/E-Architektur reicht es mitunter, SecOC innerhalb der einzelnen Subnetze zu standardisieren, während die über einen Ethernet-Backbone verbundenen Zonen-Controller ihre Kommunikation auf andere Art absichern (Bild 3). Für die Ethernet-Kommunika-

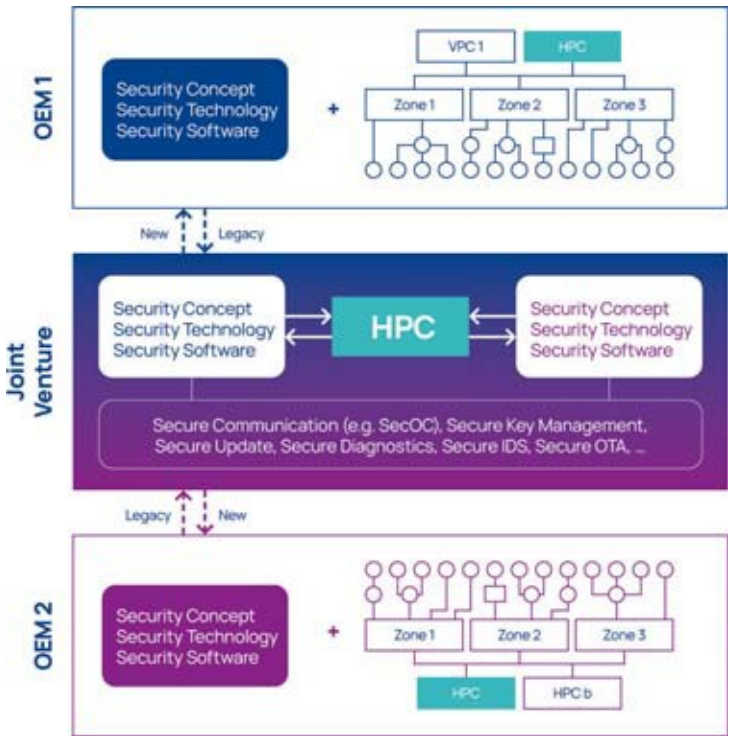

Bild 1: In einem Joint Venture entwickelte neue E/E-Architekturen bedürfen einer Übereinkunft der Partner hinsichtlich Security-Konzept, -Technologie und -Software.

Bild: ETAS

tion bietet insbesondere TLS als etablierter IT-Standard eine authentifizierte und verschlüsselte Ende-zu-Ende-Verbindung. Aus Kompatibilitätsgründen sollten die Partner sich dabei weit verbreiteter Cipher Suites bedienen. Sofern ohnehin ein KMS für SecOC existiert, kann TLS für die Authentifizierung auf vorinstallierte symmetrische Schlüssel (Pre-Shared Keys) zurückgreifen. Anderenfalls braucht es hierfür Zertifikate, wobei sicherzustellen ist, dass alle ECUs auch den Root-Zertifikaten des Partners vertrauen.

Sichere Software-Updates

Für die zunehmend Software-definierten Fahrzeuge ist die Fähigkeit, Software sicher zu aktualisieren, von zentraler Bedeutung. Die Authentifizierung von Updates erfolgt typischerweise über asymmetrische Kryptographie. Jede ECU verfügt dabei über ein Root-Zertifikat einer Public-Key-Infrastruktur (PKI), das als Vertrauensanker zur Prüfung der Signatur des Backends dient.

Je nach Partnerschaft ergeben sich hier zwei verschiedene Szenarien: Entweder werden die im Joint Venture für beide OEMs gemeinsam entwickelten ECUs, in deren jeweiligen Fahrzeugen über die jeweils eigenen Backends geupdatet. Oder es werden von den Partnern eigenständig entwickelte ECUs in einer gemeinsamen Architektur fusioniert. Entsprechend erfolgt auch die technische Anpassung entweder im Backend, das dann für unterschiedliche ECUs angepasste Signaturen erstellt. Oder sie erfolgt im Steuergerät selbst, dessen Software so erweitert wird, dass sie mehrere Algorithmen oder Schlüssel der Partner akzeptiert. Für die Wahl der geeigneten Strategie sind hier verschiedene Fragestellungen abzuwägen:

- Erlaubt der Zeitrahmen Änderungen an der Basis-Software der ECUs?
- Verfügen die ECUs über die Hardware- oder Rechenleistung, um alle Algorithmen zu unterstützen?
- Können die relevanten Schlüssel und Zertifikate dynamisch über ein Key-Management-System (KMS) eingespielt werden, oder sind sie fest in der ECU-Software verankert?
- Wie hoch ist der Aufwand für Anpassungen in den jeweiligen Backend-Systemen der Partner?

Harmonisiertes Schlüsselmanagement ist unentbehrlich

Ein harmonisiertes Key-Management-System (KMS) ist für die meisten vernetzten Security-Funktionen in der partnerschaftlich entwickelten E/E-Architektur unentbehrlich; es sorgt für die sichere Verteilung und Aktualisierung der benötigten kryptographischen Schlüssel. Jedoch gibt es im Automotive-Bereich hier kaum übergreifende Standards; das KeyM-Modul von AUTOSAR etwa spezifiziert lediglich den Umgang mit Schlüsseln innerhalb(!) eines Steuergeräts, nicht aber den übergeordneten Verteilprozess. Ein Kompromiss zwischen zwei etablierten, proprietären KMS-Lösungen der Partner ist daher technisch meist nicht realisierbar. Die Kooperationspartner müssen sich für eines ihrer bestehenden

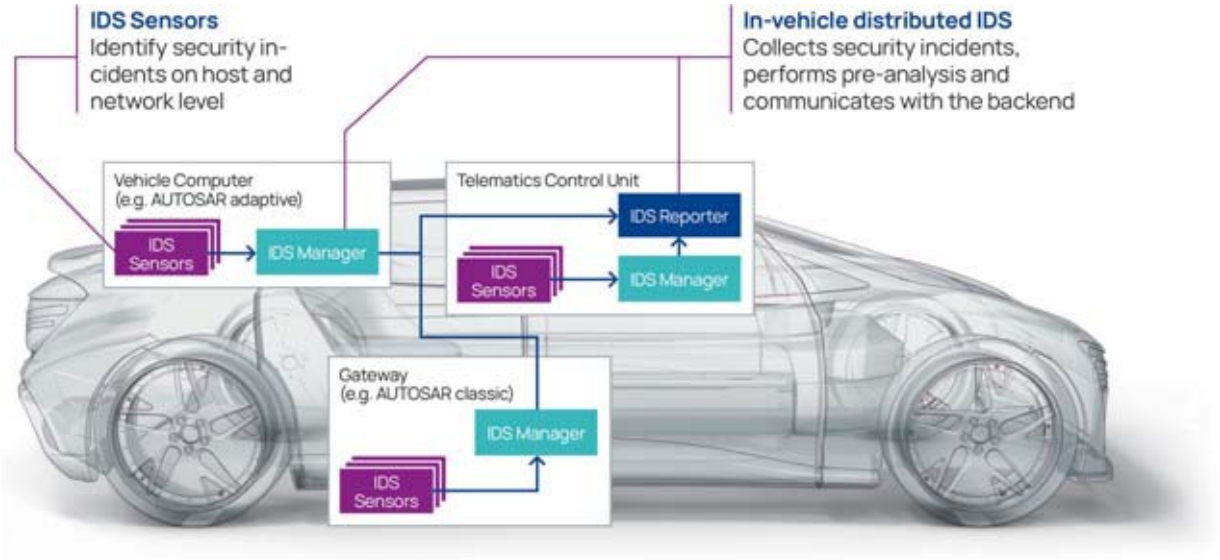

Bild 2: Bei partnerschaftlich entwickelten Architekturen sind idealerweise sowohl einheitliche Auslösebedingungen von Security Events durch die IDS-Sensoren als auch ein einheitliches Datenformat zur Weiterleitung ans Backend durch den IDS-Manager spezifiziert.

Bild: ETAS

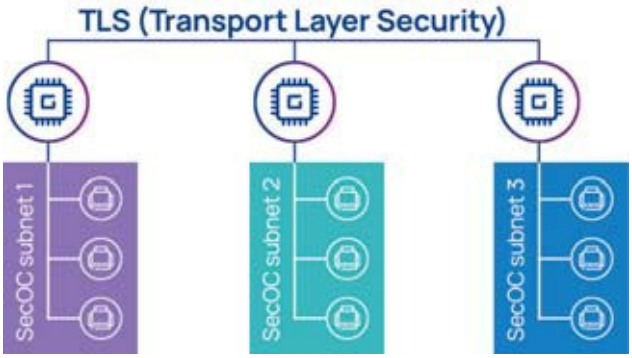

Bild 3: In zonalen Architekturen genügt zumeist eine Standardisierung per SecOC auf Subnetz-Ebene. Für den darüberliegende Ethernet-Backbone bietet TLS eine authentifizierte und verschlüsselte Ende-zu-Ende-Verbindung.
Bild: ETAS

Systeme entscheiden, oder gemeinsam ein neues definieren.

Grundsätzlich gibt es für das Key Management zwei mögliche Modelle: die externe Erzeugung des Schlüsselmaterials im Backend mit anschließender Injektion ins Fahrzeug (meist in der Produktion), oder eine dynamische Erzeugung und der Austausch von Schlüsseln direkt zwischen den Steuergeräten im Feld. Ersteres ermöglicht unter anderem die Generierung Use-Case-spezifisches Schlüsselmaterials für dasselbe Steuergerät. Letzteres bietet dagegen mehr Flexibilität in der Onboard-Kommunikation und weniger Abhängigkeit vom Backend in der Produktion. Beiden Ansätzen gemeinsam ist, dass sie einen initialen Vertrauensanker erfordern, der es den Steuergeräten ermöglicht, das Schlüsselmetrial zu authentifizieren.

Angriffserkennung vereinheitlichen

Ein Intrusion Detection System (IDS) im Fahrzeug dient dazu, potenzielle Cyberangriffe frühzeitig zu erkennen, um über das Backend Gegenmaßnahmen einleiten zu können, bevor sich ein Angriff auf die gesamte Flotte ausweitet. Dabei überwachen zahlreiche Sensoren die Subsysteme und deren Kommunikation, und melden auffällige Aktivitäten und Anomalien als „Security Events“ an die IDS-Manager in den Steuergeräten. Die wiederum prüfen und filtern die Daten, leiten sie an den zentralen IDS-Reporter im Fahrzeug weiter, der sie für eine möglichst einfache, automatisierte Analyse im Backend bereitstellt (Bild 2).

In einer partnerschaftlich entwickelten Architektur müssen die verschiedenen Bausteine und Instanzen der Angriffserkennung entsprechend gut aufeinander abgestimmt sein. So sollten die Bedingungen, unter denen ein Security-Event ausgelöst wird, sowie das Format der Event-Meldungen unbedingt einheitlich sein. Einen gemeinsamen Nenner bietet hier etwa der von AUTOSAR spezifizierte IDS-Manager, der Informationen aller Sensoren sammelt und in einem festgelegten Format weiterleitet; dabei spezifiziert AUTOSAR auch einige Security Events und ihre Auslösebedingungen.

Falls eine vollständige Harmonisierung der Angriffserkennung nicht möglich ist, sollten zumindest unterschiedliche Event-IDs oder Markierungen in den Kontextdaten verwendet werden. Dadurch erkennt das Backend, welchen der unterschiedlichen Prämissen der Partner die Meldung folgt, und kann dies bei der Analyse zusätzlich berücksichtigen.

Fazit: Mehrwert für SDV-Security

Kooperationen zur Entwicklung neuer Fahrzeugplattformen sind für OEMs mittlerweile ein probates Mittel, um im Wettlauf zum SDV zu bestehen. Damit solche Joint Ventures ihr volles Potenzial entfalten können, ohne den Cyberschutz der Fahrzeuge zu kompromittieren, muss die Cybersecurity von Anfang an als integraler Bestandteil der Zusammenarbeit verstanden werden. Eine frühzeitige Harmonisierung auf organisatorischer wie technischer Ebene ist daher unerlässlich.

Von entscheidender Bedeutung ist dabei auch die durchgängige Betrachtung der Cybersicherheit nach Produktionsstart über den gesamten Fahrzeuglebenszyklus hinweg. Schwachstellen-Management und Updates etwa sind für die Homologation nach UN R 155 und das Kundenvertrauen zwingend erforderlich.

Gerade in der gemeinsamen Bewältigung dieser Post-SOP-Aufgaben liegt eine besonders große Chance: Durch die Bündelung von Erfahrungen und Expertise können die beteiligten Partner den Fahrzeugschutz auf ein deutlich höheres Niveau heben. So entspringt der gemeinsamen Entwicklung ein echter Mehrwert für die umfassende Cybersicherheit der Software-definierten Fahrzeuge von morgen. *(na)* ■

Autoren: Dr. Christoph Stadtmüller, Engagement Manager Automotive Cybersecurity bei ETAS, Lena Steden, Principal Global Market Access bei ETAS