© ETAS

Zukunftsfeste Firewalls für zonale E/E-Architekturen

Neue Ansätze für Cybersecurity

Der Übergang von domänenzentrierten zu zonalen E/E-Architekturen mit Vehicle Computern und hohem Bedarf an Hochgeschwindigkeits-Datenkommunikation per Ethernet erfordert neue Ansätze bei deren Absicherung gegen Cybersecurity-Risiken. Ein zentraler Baustein sind dezentralisierte Firewalls, für deren Spezifikation und Konfiguration aber bisher keine verbindlichen Regeln vorhanden waren.

Dr. Michael Peter Schneider und Dr.Ing. Siddharth Shukla

Moderne Fahrzeuge sind in stark steigendem Maße durch ihre Software definiert. Damit einher geht ein rasanter Anstieg der Datenkommunikation und übertragenen Datenvolumen. Deren Übertragung in der erforderlichen – oft sicherheitsrelevanten – Geschwindigkeit verlagert sich zunehmend auf breitbandige Ethernet-Netze. Sie gewährleisten die Kommunikation zwischen Steuergeräten (ECUs), Infotainment- und Sicherheitssystemen, übertragen nahezu in Echtzeit jene Kamera- und Sensordaten als Basis für Fahrerassistenzsysteme (ADAS) und das automatisierte Fahren, sorgen für Konnektivität und ermöglichen Firmware-Updates und Ferndiagnosen. Zudem sind sie wegen der Zuverlässigkeit und des Determinismus des Ethernet-Standards ein Enabler der zeitabhängigen Vernetzung (TSN) sowie diverser Redundanz- und Failover-Mechanismen im Fahrzeug. Und nicht zuletzt sind Ethernet-Netzwerke gut skalierbar, was die Integration zusätzlicher ECUs, Sensoren oder künftig auch Vehicle Computer in die bestehende Architektur vereinfacht. Bei der zunehmenden Vernetzung und Automatisierung des Software-definierten Fahrzeugs kommt Ethernet eine Schlüsselrolle zu.

Neue Security-Anforderungen

Der fortschreitende Ethernet-Einsatz trägt aber auch zu einem weiteren Entwicklungstrend bei: Automobilhersteller (OEMs) treiben die Einführung zonaler anstelle bisher domänenspezifischer E/E-Architekturen voran. Statt E/E-Topologien logisch anhand der Funktionen zu strukturieren, zerlegen solche zonalen Architekturen (**Bild 1**) die physische Fahrzeugstruktur in Zonen wie vorne links, vorne rechts, hinten links und hinten rechts. Der Verkabelungsaufwand sinkt dadurch erheblich, was große Kostenvorteile hat. Andererseits nimmt die Komplexität im Netzwerk stark zu, wenn die bisherige Domänentrennung entfällt und ECUs mehrere Funktionen gleichzeitig übernehmen.

Exakt hier erfordert der beschriebene Paradigmenwechsel neue Ansätze in der Automotive Security: Während in bisherigen Architekturen Ethernet-Firewalls an zentralen Punkten wie Gateways, ECUs mit externen Schnittstellen oder an ECUs mit Datenverteilfunktion genügten, sind derartige Firewall-Konzepte nach dem Verschmelzen der Funktionen in zonal strukturierten Architekturen unzureichend. Vielmehr gilt es, Firewalls über unterschiedliche Layer und Zonen zu verteilen und strategisch sinnvoll in Vehicle Computer, Zonensteuergeräte sowie Ethernet-Switches und dezentrale ECUs zu integrieren.

Denn dann können Firewalls nicht nur zum zentralen Baustein für den Schutz des einzelnen Fahrzeugs, sondern darüber hinaus für die Absicherung ganzer Flotten werden. Warum dem so ist, ergibt sich aus den wichtigsten Anwendungsfällen.

Firewalls strategisch sinnvoll im Netzwerk verteilen

Vehicle Computer mit leistungsstarken Mikroprozessoren werden neue Knotenpunkte in zukünftigen E/E-Architekturen sein. Entsprechend wichtig ist es, ihren Datenverkehr umfassend zu überwachen und die jeweiligen Netzwerke als Virtual Local Area Networks (VLANs) voneinander zu trennen. Die Überwachung erfolgt per Firewall sowohl für den domänenübergreifenden als auch für den End-to-End-Verkehr. Darüber hinaus sollte die Möglichkeit zur Deep Packet Inspection gegeben sein und das Ethernet-Netzwerk per Intrusion Detection auf etwaige Angriffsversuche hin überprüft werden. Neben diesem Maßnahmenpaket für die zonalen Vehicle Computer bleiben auch in Zukunft Firewalls an den Ethernet-Switches gefragt. Netzwerktrennung in VLANs und Firewalls zur Überwachung des domänenübergreifenden Hochgeschwindigkeits-Datenverkehrs sind auch dort geboten. Zudem ist die Zugangskontrolle zum Fahrzeugserver an den Ethernet-Switches zu verorten. Des Weiteren sind Firewalls und Intrusion Detection Systeme (IDS) auf den dezentralen ECUs und Domänencontrollern gefragt, um dort Zugangskontrollen zu gewährleisten und zonale sowie auf spezifische Aufgaben wie das Laden von Elektrofahrzeugen ausgerichtete Datenbewegungen abzusichern.

Angesichts dieses Anforderungsprofils drängt sich der Gedanke auf, dass dezentrale Firewalls und IDS nicht nur die Unstimmigkeiten und Auffälligkeiten am einzelnen Fahrzeug erkennen, qualifizieren und dokumentieren können, sondern relevante Vorfälle an ein Vehicle Security Operations Center (VSOC) übermitteln sollten. Denn dort

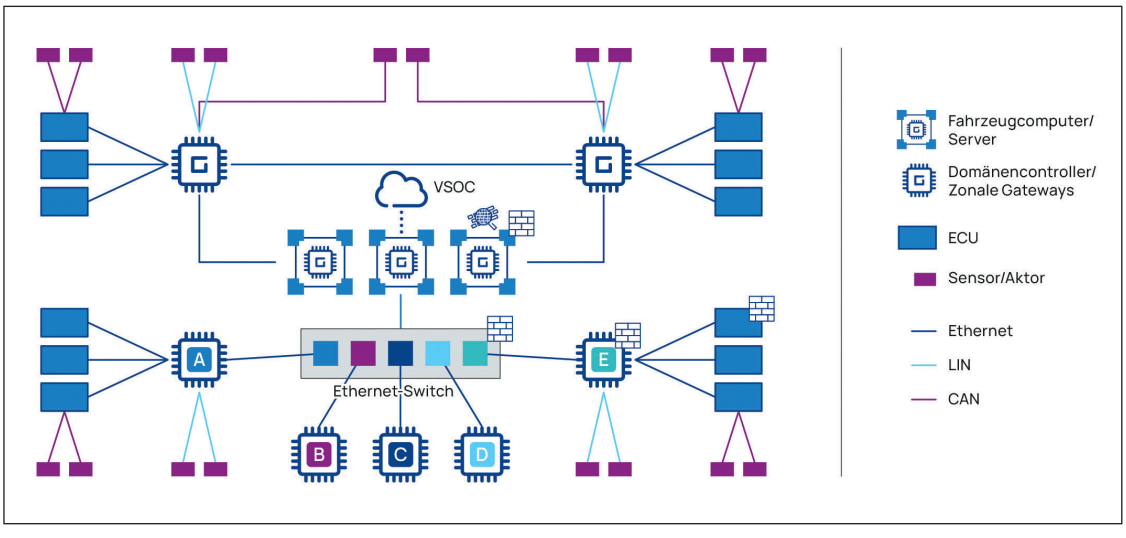

Bild 1: Automobilhersteller treiben die Einführung zonaler anstelle bisher domänenspezifischer E/E-Architekturen voran. © ETAS

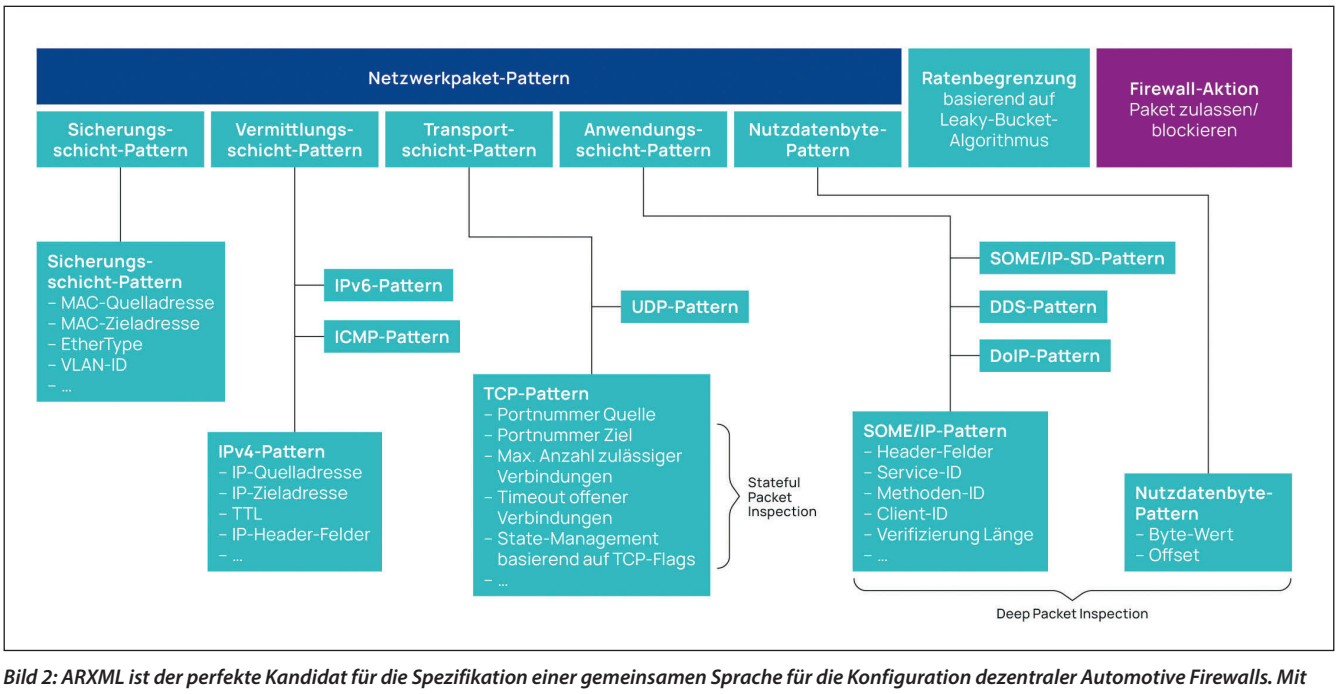

Bild 2: ARXML ist der perfekte Kandidat für die Spezifikation einer gemeinsamen Sprache für die Konfiguration dezentraler Automotive Firewalls. Mit dem Release R22–11 wurde eine schematische Konfiguration vorgestellt, die als Basis für Firewalls in AUTOSAR dienen kann. © ETAS

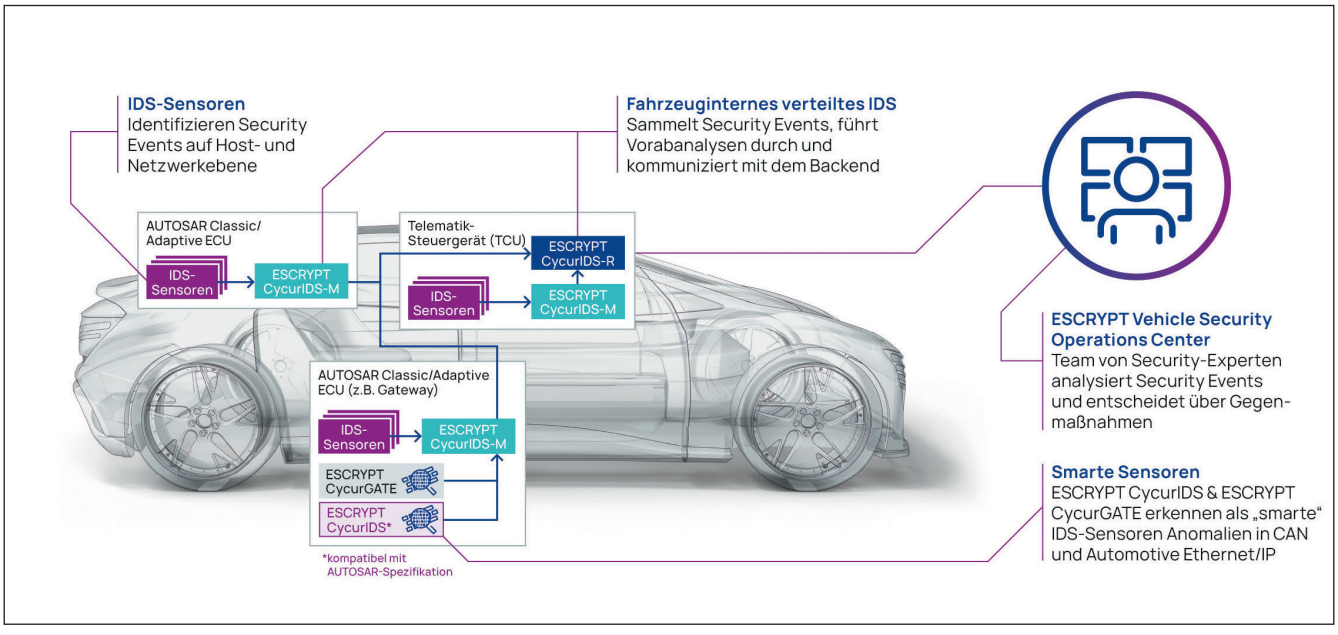

Bild 3: Firewalls sind ein Basisbaustein der Intrusion Detection Systeme, die die UN R155 zur Security-seitigen Voraussetzung für die Typgenehmigung moderner Fahrzeuge erklärt. © ETAS

könnten sie zur Grundlage für Schutzmaßnahmen werden, die in Form von Security-Updates over the Air (OTA) auf sämtliche Fahrzeuge des Automobilherstellers im Feld ausgerollt werden können. Doch um eine solche Immunisierung von Gesamtflotten umsetzen zu können, muss zunächst geklärt werden, wie genau die Firewalls und ihre Funktionen zu konfigurieren sind, welche Formate für den Austausch der Firewall-Konfigurationen nutzbar sind und welche von den Firewalls erkannten Ereignisse an das VSOC zu melden sind. Gefragt ist also eine möglichst weitgehende Standardisierung der Firewall-Funktionen, der Austauschformate für die Firewall-Konfigurationen und der Netzwerk-IDS-Anforderungen. Erst auf Basis dieser Standardisierung ist die effiziente Absicherung der zonalen E/E-Architekturen mit dezentralen Firewalls praktikabel.

AUTOSAR-Standardisierung löst aktuelle und zukünftige Herausforderungen

Diese Standardisierung hat ein Gremium, in dem ETAS maßgeblich mitgewirkt hat, unter dem Dach von AUTOSAR in die Praxis umgesetzt. Wegen ihrer hohen Akzeptanz und Verbreitung in Fahrzeugen ist AUTOSAR die ideale Plattform, zumal sich dahinter neben konkreter Steuergeräte-Software auch das Format ARXML verbirgt, das zur Konfiguration des AUTOSAR-Stacks und zum Austausch von Anforderungen zwischen Automobilherstellern und Zulieferern etabliert ist. ARXML war also der perfekte Kandidat für die Spezifikation der gemeinsamen Sprache für die Konfiguration der dezentralen Automotive Firewalls. Das Gremium hat mit dem Release R22–11 eine schematische Konfiguration vorgestellt, die als Basis für Firewalls im Standard AUTOSAR Adaptive dienen kann. Das Schema (**Bild 2**) liefert anhand der im Open-Systems-Interconnection-Referenzmodell (OSI) definierten Netzwerk-Layer ein fein aufgelöstes Netzwerk-Paketmuster, an dem sich die Praxis der Firewalls ausrichtet. Entsprechen Netzwerkpakete vorab in Allow- und Blacklists dokumentierten Mustern, führt die Firewall die zugehörige Aktion aus. Dabei liegt laut Konfigurationsschema nicht nur eine oberflächliche Header-Inspektion zugrunde, sondern bei Bedarf eine tiefgehende Paketinspektion der Protokolle in Anwendungs-Layern wie SOME/IP, DDS oder DoIP. Auch ist eine zustandsabhängige Paketprüfung vorgesehen, sei es auf Basis einer limitierten Anzahl zulässiger TCP-Verbindungen, sei es per Zustandsverwaltung anhand von TCP-Flags oder mit einer Begrenzung der Übertragungsrate von Netzwerkpaketen. Mit dieser Vielfalt an Konfigurationsmöglichkeiten deckt das Schema alle im Automotive-Bereich relevanten Firewall-Anwendungen ab.

Nach R22–11 hat das Gremium mit dem Release R23–11 eine Lösung für Firewalls in AUTOSAR Classic und AUTOSAR Adaptive vorgestellt, die zusätzlich moderne Switches einschließt. Denn dank eigener Mikrocontroller sind diese in der Lage, komplexe Netzwerk-Paketprüfungen auszuführen. Hierfür ist eine an die begrenzten Ressourcen des Switch-Mikrocontrollers adaptierte Version von AUTOSAR Classic erforderlich. Auch sollte die Inspektion der Netzwerkpakete nicht allein dem Mikrocontroller aufgebürdet, sondern größtenteils an den Switch-Core delegiert werden. Denn dort ist diese Aufgabe dank der optionalen Hardware-Beschleunigung besser aufgehoben. Um diese Anwendung in die Praxis umsetzen zu können, sind im AUTOSAR-Firewall-Modul entsprechende Schnittstellen zum Switch-Core und Abläufe gemäß der für die Auslastung von Managed Switches vorgesehenen Ternary Content Addressable Memory-Regeln (TCAM) verankert.

Firewall als Basisbaustein eines zukunftsfesten Security Monitoring

Die grundlegende Funktion von Automotive Firewalls ist es, potenziell maliziöse Pakete von ECUs und Vehicle Computern fernzuhalten. Daneben können sie als stille Detektive den Netzwerkverkehr überwachen und Angriffe identifizieren, die sich die Fahrzeugvernetzung zunutze machen. In dieser Funktion sind Firewalls ein Basisbaustein der Intrusion Detection Systeme (IDS), die die UN R155 zur Security-seitigen Voraussetzung für die Typgeneh-

migung moderner Fahrzeuge erklärt (**Bild 3**). AUTOSAR greift das im Release R20–11 auf, das die Einführung eines IDS-Managers (IdsM) vorsieht. Dafür ist eine IDS-Sensorik gefordert, die Security-relevante Ereignisse (SEvs) sammelt, qualifiziert und sie für die weitergehende Analyse an ein VSOC übermittelt.

In ihrer Monitoring-Funktion erfüllen dezentrale Firewalls exakt diese Aufgabe: Sie sind IDS-Sensoren, die Security-Ereignisse im Netzwerk identifizieren und an den IdsM melden. Ihr großer Vorteil ist die Tiefe und Breite, mit der sie den Netzwerkverkehr über alle Zonen und Layer hinweg überwachen – von der Inspektion der Paket-Header bis zur In-depth-Analyse der Inhalte und Protokolle. Damit sind die dezentralen Firewalls in der Lage, jegliche Angriffe zu erkennen, die über einen der häufigsten Angriffsvektoren durchgeführt werden: das Netzwerk. Weil sie verschiedene Protokolle über mehrere OSI-Layer hinweg abdecken, erkennen sie obendrein ein breites Spektrum netzwerkbasierter Angriffe einschließlich solcher auf die Transportschicht (wie SYN/ACK Flood) und Dienstebene (z. B. auf SOME/IP). Genau zu diesem Zweck hat das AUTOSAR-Gremium einen Satz von 16 Security Events (SVEvs) spezifiziert, die das Firewall-Modul im Falle möglicher Angriffe aktivieren.

Ausblick

Dank der nun erfolgten Ausgestaltung der Firewall-Konfigurationen in den Regelwerken von AUTOSAR Classic und Adaptive können Firewalls zukünftig eine Schlüsselrolle im wirksamen Security-Monitoring einzelner Fahrzeuge und darüber hinaus für die Immunisierung ganzer Flotten übernehmen. Gerade mit Blick auf den Wandel von domänenspezifischen zu zonalen E/E-Architekturen und den dadurch ausgelösten Bedarf an dezentralen, im ganzen Fahrzeugnetzwerk verteilten Firewalls war für diese Standardisierung grundlegende Basisarbeit zu leisten. Mit den zwei Releases R22–11 und R23–11 sind die Grundlagen dafür gelegt, dass Automotive Firewalls zu einem Basisbaustein für künftige IDS-Architekturen im Fahrzeug werden können. Daneben legt die AUTOSAR-Firewall-Standardisierungsinitiative mit der universelle Sprache ARXML die Basis für ein herstellerübergreifendes Verständnis von Firewall-Konfigurationen und für deren Austausch. Die Initiative ebnet damit den Weg zur Umsetzung der UN-Regulierung R155, die ein wirksames IDS-Management zur Voraussetzung zukünftiger Typgenehmigungen macht. ■ (eck)

www.etas.com

Dr. Michael Peter Schneider ist Lead Technical Officer AUTOSAR Security bei der ETAS GmbH in Stuttgart. © ETAS

Dr.Ing. Siddharth Shukla ist Senior Product Manager für das Produktfeld Onboard Security bei der ETAS GmbH in Stuttgart. © ETAS