



AUTOMOTIVE SECURITY

Angriffsschutz für Infotainment-Integration

Die nächste Generation von Infotainment-Systemen im Auto wird Features anbieten, die die Hersteller in puncto Funktionssicherheit und Angriffsschutz vor große Herausforderungen stellen. Dieser Artikel beleuchtet einige dieser Sicherheitsfragen und stellt eine Software-Architektur vor, die eine Antwort auf genau diese Fragen bietet.

Die Vernetzung des Fahrzeugs mit der Außenwelt wird zum Wettbewerbsfaktor für Automobilhersteller. Deshalb müssen sich Kfz-Infotainment-Systeme zunehmend öffnen und sowohl mit dem Bordnetz im Fahrzeug als auch mit der Außenwelt und der „Cloud“ interagieren. Moderne automobiler Online-Dienste erfordern sogar eine Interaktion zwischen der „Cloud“ und der Fahrzeugelektronik. Diese Anbindung birgt das Risiko, dass Angreifer das Kfz-System stören oder gar manipulieren.

Der Umfang dieses Risikos steht in direktem Verhältnis dazu, wie weit sich ein System öffnet und wie komplex seine Interaktion mit anderen Systemen ist. So beansprucht z. B. das Abschließen der Wagentür, Starten der Klimaanlage oder Laden der Batterie eines Elektrofahrzeuges über Telekommunikation nur eine relativ einfache Interaktion zwischen Außenwelt und Bordnetz. Diese Features werden schon bald eine Selbstverständlichkeit sein. Wenn dagegen Software integriert werden soll zur Fehlerdiagno-

se oder Überwachung des Fahrzeugzustandes durch Vernetzung mit entsprechenden Geräten, dann sind dafür sehr komplexe Interaktionen zwischen dem einzelnen Gerät im Auto und der Außenwelt erforderlich.

Und noch komplizierter wird es, wenn der Kunde das Infotainment-System seines Autos selbstständig aktualisieren und neue Apps installieren kann. Dringt dabei eine zerstörerische Software in das Infotainment-System, kann sie über den Fahrzeug-Bus das Software-System befallen und große Gefahr für den Fahrer bedeuten. Zum Schutz davor können die Hersteller zunächst kontrollierte Datenquellen bereitstellen und die Datenübertragung nur über kontrollierte Kommunikationsmechanismen zulassen. Mittelfristig allerdings werden die Kunden Upgrades und Apps von Online-Plattformen herunterladen und installieren. Mehr noch, sie werden Apps installieren, die aus potenziell unzuverlässigen Quellen stammen. Solche Apps können dem Fahrer nur dann wirklich nützen, wenn sie auf kontrollierte Weise mit dem Bordnetz im Auto kommunizieren. Das

heißt, die App auf dem Infotainment-System erhält kontrollierte Zugriffsrechte auf die Daten, die auf dem Fahrzeug-Bus liegen. Das Security-Thema ist somit Schutz und Chance zugleich im Wettbewerb um das kundenfreundlichste Auto von morgen.

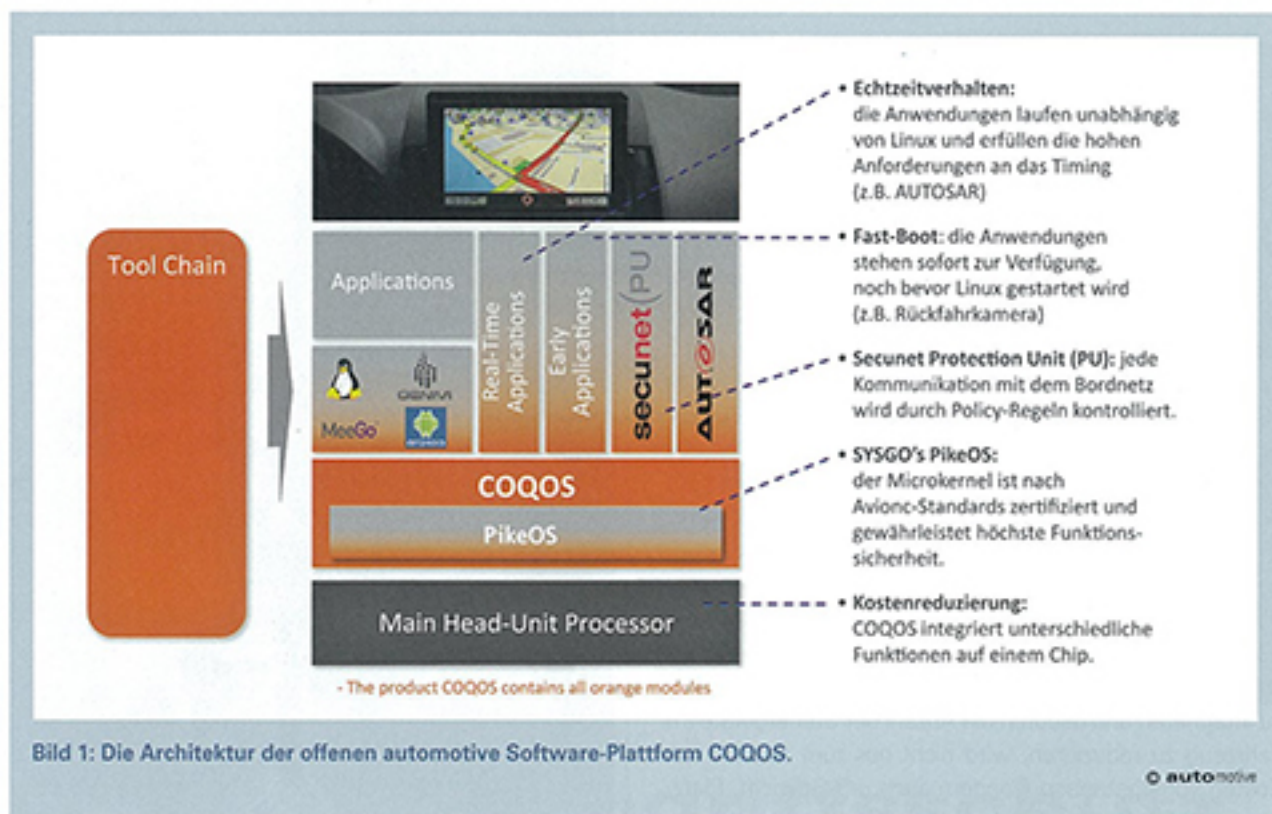
Infotainment und Safety

Ein ganz anderer Aspekt ist die Erwartung, dass die neue Generation von Infotainment-Systemen es auch mit Safety-relevanten Funktionen zu tun haben wird. Hersteller und Zulieferer möchten für ihre processorintensiven Fahrerassistenz-Funktionen wie z. B. Parkassistent, Rückfahrkamera oder Lane-Assistent die hohen Rechnerleistungen der Infotainment-Hardware nutzen. Dazu wird die Software auf demselben Chip mit der Infotainment-Software integriert. Das bedeutet, dass die Hardware-Ressourcen einer Head-unit aufgeteilt werden müssen zwischen reinen Infotainment-Funktionen und Funktionen, die Einfluss auf die Sicherheit des Fahrens haben. Diese Notwendigkeit, automotiv Software zusammen mit Infotainment-Systemen zu integrieren und dadurch die Anzahl der Steuergeräte im Fahrzeug zu reduzieren, wird nicht nur zum Sparen von Kosten vorangetrieben, sondern auch um Gewicht, Platz, Komplexität, Treibstoffverbrauch und den allgemeinen Energieverbrauch des Autos zu reduzieren. Auch die Mensch-Maschine-Schnittstelle wirft eine Safety-Frage auf. Sie befindet sich typischerweise im Infotainment-System, wird aber auch für sicherheitsrelevante Funktionen angewandt werden. Ein naheliegendes Beispiel dafür ist das Display in der Mittelkonsole, auf dem das Navigationssystem läuft. Hier sollen die Bilder der Rückfahrkamera angezeigt werden und zwar zuverlässig und nur wenige Sekunden nach dem Start. Diese Funktion erhöht die Sicherheit des Autofahrers erheblich und wird in den USA sogar bald Vorschrift sein. Mittelfristig werden dann voll digitalisierte Armaturenbretter sowohl die Karte des Navigationssystems als auch den Tachometer und die Warnlampen abbilden. Es gibt dann also nur noch ein gemeinsames Display für Infotainment und sicherheitsrelevante Funktionen. Das zwingt die Hersteller von Infotainment-Systemen einen Weg zu finden, um ihre Produkte auf die Norm 26262 oder ASIL B abzustimmen.

Architekturvorschlag

Vorgestellt wird eine Architektur, die all diese Ansprüche an Funktionssicherheit und Angriffsschutz berücksichtigt. Gleichzeitig bietet sie eine kostengünstige und skalierbare Lösung und erfüllt die automotiv Anforderungen. Das Konzept dieser Architektur (**Bild 1**) besteht aus folgenden Elementen:

- Ein zertifizierter Microkernel, der die funktionssichere und gegen Angriffe geschützte Integration von mehreren Partitionen auf einem Steuergerät ermöglicht.
- Ein Betriebssystem aus dem Bereich der Unterhaltungselektronik (wie z. B. Linux oder Android), das auf einem Mikro-Betriebssystem virtualisiert läuft.
- Automotive Software, die Echtzeitanforderungen entspricht oder ein gesamter AUTOSAR-Stack innerhalb einer Partition.



- Regelbasierte Firewalls, die die Interaktion kontrollieren und dafür in jeweils eigenen Partitionen laufen.

Das Unternehmen OpenSynergy hat diese Architektur mit seiner Plattform COQOS umgesetzt. Alle aufgezählten Elemente sind in diesem Betriebssystem zusammengeführt, sodass ein oder mehrere Betriebssysteme wie Linux oder Android auf einem Infotainment-System ausgeführt werden können. Durch das Virtualisierungskonzept können die Betriebssysteme jeweils in ihrer Sandbox laufen. Es ist sichergestellt, dass diese Betriebssysteme niemals auf Hardware zugreifen können, auf die sie nicht zugreifen dürfen. COQOS unterstützt generische Linux-Kerne und kann verwendet werden, um GenIVI-konforme System zu erstellen. Außerdem unterstützt COQOS Android als offene Applikations-Plattform.

Sichere Integration

Zusätzlich umfasst COQOS ein komplettes AUTOSAR-Framework. Die von AUTOSAR festgelegten Anforderungen sind faktisch zum Standard für Embedded Systeme in Steuergeräten geworden. Das Framework bildet einen idealen Rahmen für Kfz-spezifische Funktionen in Infotainment-Systemen, wie z. B. die Integration mit dem Bordnetz (z. B. CAN) und mit Diagnosefunktionen. Echtzeit- und sicherheitsrelevante Applikationen können dann entweder auf AUTOSAR-Software-Komponenten laufen oder direkt in separaten Partitionen ausgeführt werden.

Um den Sicherheitsanforderungen hinsichtlich der Funktionssicherheit und des Angriffsschutzes bei der Infotainment-Integration zu entsprechen, haben die SYSGO AG und die secunet Security Networks AG als Unternehmenspartner von OpenSynergy zwei entscheidende Elemente zu COQOS hinzugefügt:

SYSGO liefert den PikeOS Microkernel, der direkt auf der Hardware ausgeführt wird. Die Teilungs- und Schutzfunktionen des Microkernel garantieren die sichere Integration der Partitionen auf einem einzigen Prozessor (sowohl Single-Core als auch Multi-Core). PikeOS wurde speziell für den Einsatz in sicherheitskritischen Bereichen entwickelt. Somit sind PikeOS-Projekte zertifizierbar nach sicherheitskritischen Standards wie DO-178B, IEC61508, EN 50128, MILS, CC EAL. Aufgrund seiner Zertifizierung nach höchsten Sicherheitsstandards der Luftfahrttechnik wird PikeOS unter anderem im Airbus A350XWB und im A400M eingesetzt. Da der Microkernel in diesem extrem sicherheitskritischen Umfeld Anwendung findet, ist er geeignet, die Anforderungen zu erfüllen, die sich aus der Norm ISO 26262 ergeben. Das Forschungsprojekt „VirtuOS“ (Virtuelle Architekturen in Automotiven Softwaresystemen) befasst sich derzeit mit der Vergleichbarkeit dieser Normen. Am Beispiel von SYSGO's Microkernel wird geprüft, in wie weit PikeOS durch das Erfüllen des Sicherheitsstandards der Avionik auch den Anforderungen der ISO 26262 entspricht. OpenSynergy führt das Projekt zusammen mit der TU Berlin und dem Fraunhofer Institut durch. secunet Security Networks ergänzt die Plattform COQOS mit der Protection Unit (PU). Diese Einheit läuft in ihrer eigenen isolierten Partition. Ihre Aufgabe ist es, die Kommunikation zwischen der Infotainment-Partition und der automotive Partition zu kontrollieren.

Aus den Spezifikationen der Automotive Systeme werden Policy-Regeln in der PU abgeleitet. Die PU schützt die Softwaresysteme, indem sie das komplette Kommunikationsverhalten zwischen Apps auf dem Infotainment-System und den Fahrzeugfunktionen beobachtet und mit den Policy-Regeln vergleicht. Jede Kommunikation, die von den Regeln abweicht, wird erkannt. So auch schadhafte Kom-

munikationsverhalten durch Viren, Würmer, Trojaner, DoS- und Buffer-Overflow-Angriffe. Um die Bestandteile eines Steuergeräts vor Beschädigung zu schützen, neutralisiert das System die Auswirkungen der erkannten Angriffe. Die Basis dafür bildet die isolierte Partition, in der die PU implementiert ist. Nur diese Partition verfügt über sichere und dedizierte Kommunikationsschnittstellen zu den automotiven Softwaresystemen. Zusätzlich fragt das Infotainment-System bei der PU Signaturverifikationen ab, bevor der User eine App installieren kann. Damit sind die Signaturprüfung und die dafür benötigten kryptografischen Schlüssel dem direkten Zugriff aus dem Infotainment-System entzogen.

Fazit

Ob die vorgestellte Architektur alle Probleme lösen kann, die in der Einführung des Artikels angedeutet wurden, hängt auch von den Möglichkeiten der Hardware ab, auf der sie ausgeführt wird. Besonders wenn komplexe Peripherien wie z. B. das Display aufgeteilt werden müssen in kritische und unkritische Informationen, muss das System-on-Chip ein entsprechendes Basis-Hardware-Feature enthalten, das dies zulässt. OpenSynergy erwartet aber, dass die neue Generation von Infotainment-Hardware zusätzliche Features bereitstellt, um Hardware zu teilen, sichere Boot-Chains zu implementieren und die Separierung von Betriebssystemen effizienter zu machen.

Aus Sicht von OpenSynergy gibt es keine konkurrenzfähigen Alternativen zu der vorgeschlagenen Architektur. Ein naheliegender Ansatz etwa ist der, geteilte Hardware zu verwenden und die beschriebenen unterschiedlichen Softwaresysteme jeweils auf verschiedene Prozessoren zu installieren. Viele herkömmliche Head-Units enthalten mindestens zwei Prozessoren: einen um das Infotainment-System auszuführen und einen für die Schnittstelle zum Bordnetz. Dieser Ansatz ist vergleichsweise unflexibel,

macht die Hardware noch komplexer, treibt die Entwicklungskosten in die Höhe und führt nicht dazu, die Anzahl der Steuergeräte im Fahrzeug zu senken.

Ein anderer Ansatz sieht vor, die Betriebssysteme der Unterhaltungselektronik zu modifizieren und an die automotive Welt anzupassen. So könnte z. B. ein Linux-Betriebssystem soweit optimiert werden, dass die Startzeiten fast den Kfz-Anforderungen entsprechen. Alternativ könnte ein Linux-Betriebssystem so erweitert werden, dass es bessere Echtzeit-Eigenschaften besitzt und Ansprüchen an Funktionssicherheit und Angriffsschutz gerecht wird. Diese Vorgehensweise hat aber zwei Nachteile: Erstens ist sie ungeeignet, um die strengen Anforderungen wie ISO 26262, ASIL B oder Fastboot zu erfüllen. Auch aus Sicht der Security ist dieser Ansatz nicht zukunftsfähig, da hier keine ausreichend hohen Security-Standards, z. B. EAL7 nach Common Criteria, erreicht werden können. Zweitens widerspricht sie den ursprünglichen Absichten für die Verwendung von Software aus der Consumer-Elektronik im Automobilbereich. Mit der Schaffung fahrzeugspezifischer Derivate aus der Unterhaltungselektronik ist niemandem gedient. Ziel muss es sein, bestehende Software-Lösungen aus der Unterhaltungselektronik wiederzuverwenden und diese schnelllebige Welt mit ständig neu erscheinenden Features und Feature-Updates funktions- und angriffssicher in das Auto zu integrieren. (oe)



Dr. Stefaan Sonck Thiebaut ist Geschäftsführer der OpenSynergy GmbH in D-10245 Berlin.

OpenSynergy GmbH
www.opensynergy.com