Virtuelle Steuergeräte in Serienfahrzeugen?

AUTOREN

Michael Hauser ist Teamleiter Software-Entwicklung bei **Bosch Automotive Electronics** in Stuttgart.

Dr. James Dickie ist Produktmanager RTA-Solutions bei **ETAS Ltd** in York, Großbritannien.

Dr. Nigel Tracey ist General Manager bei **ETAS Ltd** in York, Großbritannien.

ETAS Lightweight Hypervisor sorgt für Flexibilität, Effizienz und Sicherheit

Die Automobilindustrie setzt zunehmend auf agile Software-Entwicklung. Bedenkenlos sollen Kunden softwaregesteuerte Fahrzeugfunktionen upgraden oder updaten können. Das setzt eine strikte Trennung der einzelnen Softwarefunktionen voraus. Der Trend bei der Hardware weist jedoch in die entgegengesetzte Richtung: Auf zentralen Steuergeräten laufen immer mehr Funktionen. Um diesen Widerspruch zu lösen, setzt Bosch Automotive Electronics den neuen Lightweight Hypervisor von ETAS ein.

Nach drei unfallfreien Jahren ist es so weit. Leons Eltern loggen sich beim OEM ein. Die softwaregesteuerte Leistungsdrosselung seines Autos, das er zum Führerschein bekommen hat, wird endlich entfernt. Zudem bekommt er das neue Multimedia-Paket aufgespielt, das er zur Hälfte selbst bezahlt.

Nachträgliche Funktionsupgrades und fortlaufende (Over-the-Air-)Updates setzen voraus, dass Modifikationen keinesfalls andere Software in Mitleidenschaft ziehen. Doch wie lässt sich das gewährleisten, wenn der Trend gleichzeitig zur Konzentration von immer mehr miteinander vernetzten Funktionen auf wenigen, zentralen Steuergeräten geht? Ist es in einem solchen Umfeld überhaupt möglich, vorab mit Tests die funktionale Sicherheit des Gesamtsystems nach den Upgrades und Updates zu validieren und zu verifizieren? Schon diese beiden Fragestellungen zeigen, dass es gelingen muss, Softwarefunktionen sicher voneinander zu entkoppeln.

Praktikable Partitionierung ist gefragt

Nicht nur unter dem Aspekt der funktionalen Sicherheit ist diese Entkopplung gefragt. Sie vereinfacht auch die Workflows in der Entwicklung, wenn Software unterschiedlicher Hersteller auf ein und demselben Steuergerät betrieben wird. Zudem sorgt die Trennung dafür, dass Steuergeräte in Zeiten zunehmender Cyberkriminalität schwerer angreifbar sind. Hat sich ein Hacker Zugang zu einer Funktion verschafft,

stellt der Hypervisor eine weitere hohe Hürde für ihn dar. Eine wenig reizvolle Aussicht für die Cyberkriminellen, die ja einen größtmöglichen Schaden anrichten wollen.
Um die Entkopplung zu realisieren, sind verschiedene Ansätze denkbar. So könnte man Softwarefunktionen strikt auf jeweils eigene Steuerungshardware verteilen. Doch sowohl die Hardwarekosten als auch die Systemkomplexität sprechen dagegen. Realitätsnäher ist eine auf AUTOSAR basierende Architektur mit definierten Partitionierungs- und Separierungskonzepten.
Auf dieser Basis ist es möglich, Upgrades einzelner Funktionen zu realisieren und dabei die Beeinträchtigung weiterer Funktionen auszuschließen. So ist gewährleistet, dass die Modifikation einer Funktion keine umfassende Re-Validierung sämtlicher Software auf dem betreffenden Steuergerät erfordert. Um die AUTOSAR-Konzepte umzusetzen, sind jedoch Erweiterungen notwendig.

Lösungsansatz Hypervisor – aber wie?

Hier bietet sich der Einsatz eines Hypervisors an. Er partitioniert ein einzelnes Steuergerät in diverse virtuelle Maschinen (VM). Obwohl die Funktionen faktisch auf demselben Steuergerät laufen, wähnt sich die jeweilige Software in einem Zustand, in dem es für jede Funktion eine eigene Hardware gibt. Die Funktionen sind so strikt entkoppelt, dass sie ohne komplette Re-Validierung einzeln modifiziert werden können – und ihre verschiedenen Hersteller schon in der Entwicklung des Steuergeräts unabhängig von allen anderen arbeiten können. Softwarefehler oder böswillige Eindringlinge bleiben lokal auf eine einzelne virtuelle Maschine begrenzt.
Und es wird möglich, Software mit verschiedenen ASIL-Sicherheitseinstufungen (Automotive Safety Integrity Level) von der niedrigsten Stufe QM bis zur höchsten Anforderung ASIL D auf ein und demselben Steuergerät zu betreiben.
Bei allen Vorteilen kommt es bei einer Hypervisor-Lösung jedoch auf die Umsetzung an. Ohne Anpassung an das spezifische Umfeld im Fahrzeug droht Ungemach. So braucht ein Hypervisor üblicherweise ein eigenes Speichermanagement sowie einen sogenannten Hypervisor-Privilege-Modus, der die Zugriffsberechtigungen regelt. Dieser ist bei klassischen Ausführungen dreistufig: der Hypervisor selbst, die Basissoftware und die Applikationsfunktionen. Doch sowohl das entsprechende Speichermanagement als auch der dreistufige Privilege-Modus wird von heute eingesetzten Fahrzeug-Mikrocontrollern nicht unterstützt. Dies stand dem breiten Einsatz der Hypervisor-Technologie im Automobil bisher noch entgegen.
Bosch Automotive Electronics – Body Electronics (AE-BE) ist es in einem Projekt für einen großen OEM nun gelungen, die genannten Problemfelder mit dem ETAS Lightweight Hypervisor (ETAS RTA-LWHVR) zu entschärfen. Der optimierte Automotive-Hypervisor hat nur noch einen Speicherbedarf von 5 Kilobyte (kB) und die Zugriffszeiten konnten um Faktor vier bis fünf verbessert werden. Die neue Lösung ermöglicht, dass es zu keinerlei Beeinflussungen zwischen den virtuellen Maschinen kommt.
Im konkreten Projekt war ein zentrales Body-Steuergerät in elf virtuelle Maschinen partitioniert, die jeweils für Software von unterschiedlichen Zulieferern reserviert waren. Die ASIL-Einstufung reichte dabei von QM bis B.

Lightweight Hypervisor geht über AUTOSAR hinaus

Trotz der Menge und Heterogenität der Softwarefunktionen verlief deren per Lightweight Hypervisor gekapselter Betrieb völlig problemlos. Dies gelang, weil die virtuellen Maschinen zwar auf den gemeinsamen Speicher zugreifen, die Zugriffe und die Laufzeiten auf dem Kern aber klar geregelt sind.
Möglich wird die hohe Performance der Lösung durch Aufteilen der Rechnerkerne: einen Master Core und die Applikations-Cores. Während dem Master Core das Hardwaremanagement sowie der Betrieb der zentralisierten Basissoftware und einiger Software-Applikationen zukommt, beherbergen die Applikations-Cores die strikt getrennten virtuellen Maschinen (siehe Bild 1) – wahlweise mit aufgeteilten Laufzeitumgebungen (RTE) gemäß AUTOSAR oder auch mit nicht-AUTOSAR-konformer Software – und das auf ein und demselben Steuergerät.
Wichtig bei diesem Ansatz ist die entsprechende Inter-Core-Kommunikation (ICC). Sie wurde von Bosch AE-BE entwickelt. Funktionen können zusätzlich zur ohnehin garantierten Ausführungszeit weitere Zeitbudgets anfordern, ohne dass es zu Abstrichen bei der Ausführung anderer Funktionen kommt (siehe Bild 2). Die Echtzeitanforderungen sind also jederzeit gewährleistet.
Bei hohem Laufzeitbedarf, welcher die eigene Kapazität zu überlasten droht, können die virtuellen Maschinen beim Hypervisor anfragen, ob sie vorübergehend auf zusätzliche vorgehaltene Laufzeitfenster zugreifen können. In diesem Fall merkt der Hypervisor die virtuelle Maschine in einer Warteschleife vor. Ist ein Laufzeitfenster frei, erlaubt er der ersten virtuellen Maschine in der Schleife,

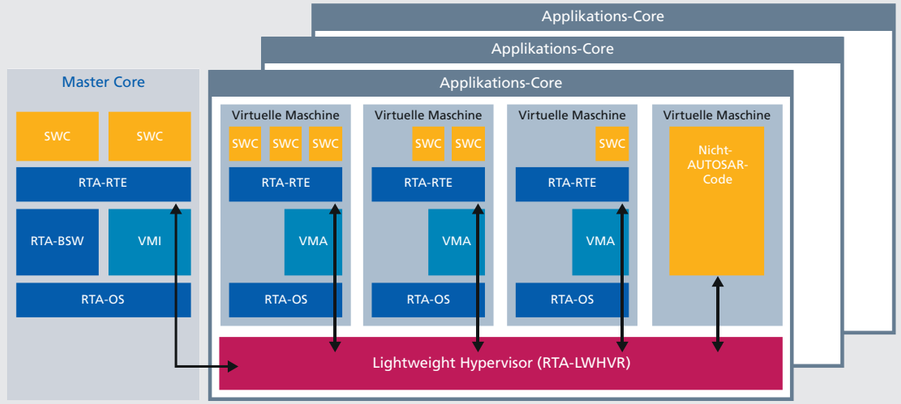

Bild 1:
Schematischer Aufbau eines Steuergeräts mit dem Lightweight Hypervisor RTA-LWHVR.

RTA-BSW AUTOSAR-Basissoftware
RTA-OS Betriebssystem
RTA-RTE Laufzeitumgebung
SWC Softwarekomponente in gesicherter Anwendung
VMA Adapter zur virtuellen Maschine
VMI Virtuelle Maschinenschnittstelle
ICC (Inter-Core-Kommunikation)
VM Virtuelle Maschine

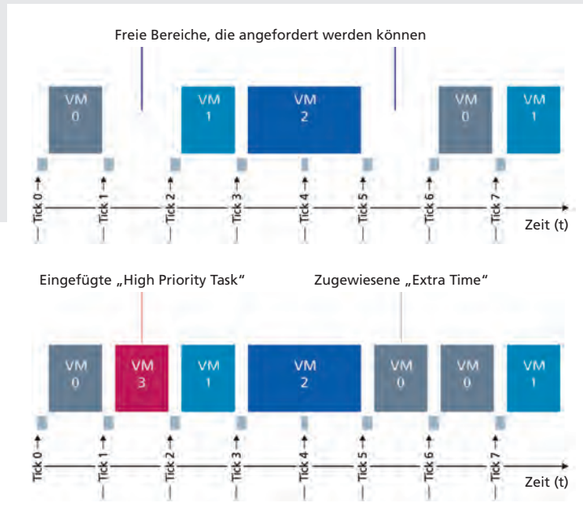

Bild 2: Zeitmanagement in einem Applikations-Core.

dieses zu nutzen. Durch dieses Vorgehen werden die Störungen durch eine hohe Systemlast minimiert. Jede virtuelle Maschine kann jedoch nur die Reservierung eines Fensters anfordern. So wird verhindert, dass eine fehlerhafte oder gehackte virtuelle Maschine die Kontrolle über das System erlangt.

Heute verfügbare, zukunftsfähige Lösung

Dank des gegenüber des klassischen Hypervisors drastisch reduzierten Overheads mit nur 5 kB Speicherbedarf und einem auf 5 Prozent der verfügbaren Kernkapazität reduzierten Leistungsbedarf, fügt sich der RTA-LWHVR problemlos in die spezifischen Randbedingungen für Embedded Systeme im Automobil ein. Er bietet volle Flexibilität für eine Vielzahl an Anwendungen und ist für zahlreiche Mikrocontroller verfügbar. Dabei gewährleistet er eine ebenso zuverlässige wie leistungsfähige Partitionierung von Steuergeräten, auf denen damit künftig Software unterschiedlicher Hersteller und Sicherheitsklassen betrieben werden können. Dank intelligenter Inter-Core-Kommunikation und strikter Kapselung können softwaregesteuerte Funktionen unabhängig voneinander entwickelt und – auch bei Fahrzeugen in Kundenhand – jederzeit ohne aufwendige Re-Validierung des Gesamtsystems modifiziert werden. Damit legt der Lightweight Hypervisor eine abgesicherte Basis für agile Software- und Funktionsentwicklung in der Automobilindustrie, die obendrein dynamische Security-Systeme mit regelmäßigen bedarfsgerechten Sicherheitsupdates möglich macht. Individuellen Konfigurationen und nachträglichen Upgrades von Fahrzeugen, wie bei Leon und seinen Eltern, steht damit nichts mehr im Wege.