Strikte Trennung erforderlich

Partitionierung ermöglicht sichere Steuergerätesoftware-Updates im Feld

Nachträgliche Funktionsupgrades und Over-the-Air-Updates bringen neue Herausforderungen für Autohersteller und Zulieferer mit sich. Um für die notwendige Sicherheit zu sorgen, bietet sich der Einsatz eines Hypervisors bei der Steuergerätesoftware an. Jetzt ist eine speziell für Automotive-Steuergeräte geeignete Version verfügbar.

Autoren: Dr. Alexander Leonhardi, Dr. Gary Morgan, Dr. James Dickie

Für Autokäufer kann die agile Software-Entwicklung mit Updates im Feld einen echten Mehrwert bieten. Statt schon beim Kauf alle Bedürfnisse vorausplanen und alle Wünsche erfüllen zu müssen, können Sie ihr Fahrzeug nach und nach erweitern oder verändern. Beispiele dafür sind Multimedia-Pakete, Navigationssoftware oder eine softwaregesteuerte Leistungsdrosselung, wenn sich der Nachwuchs mit frisch erworbenem Führerschein ans Steuer setzt.

Für die Hersteller der Fahrzeuge, Steuergeräte und Steuergerätesoftware bringen die nachträglichen Funktionsupgrades und fortlaufende (Over-the-Air)-Updates dagegen neue Herausforderungen und Risiken mit sich. Gemeinsam gilt es zu gewährleisten, dass die Modifikationen keinesfalls andere, möglicherweise sicherheitsrelevante Softwarefunktionen in Mitleidenschaft ziehen, die auf demselben Steuergerät laufen. Der Trend zur Konzentration von immer mehr miteinander vernetzten Funktionen auf wenigen, zentralen Steuergeräten macht die Aufgabe nicht leichter. Das wirft eine grundsätzliche Frage auf: Wie ist es unter den gegebenen Bedingungen überhaupt wirtschaftlich möglich, in Tests vorab zu validieren und zu verifizieren, sodass die funktionale Sicherheit des Gesamtsystems nach den Upgrades und Updates gewährleistet bleibt?

Praktikable Partitionierung ist gefragt

Klar ist, dass verschiedene Firmen Softwarefunktionen zu ein und demselben Steuergerät beisteuern. Sie müssen sich darauf verlassen können, dass ihre jeweiligen Softwaremodule einander nicht stören und dass etwaige Fehler eines Herstellers nicht auf die anderen zurückfallen können. Wünschenswert wären also klar abgesteckte, voneinander entkoppelte Bereiche, damit jedes Unternehmen nur für den reibungslosen Betrieb der eigenen Software verantwortlich wäre – inklusive aller Tests, die in den gültigen Safety-Standards festgelegt sind. Bei Veränderungen nach dem Produktionsbeginn wäre die Verantwortung ebenfalls auf diesen einen Bereich

beschränkt. Eine solche „Freedom-of Interference“ wird auch von den Safety-Standards gefordert, ist aber mit klassischen Architekturen auf einem Steuergerät nur schwer nachzuweisen.

Nicht nur unter dem Aspekt der Haftung und der funktionalen Sicherheit ist eine solche Entkopplung geboten. Sie vereinfacht auch die Workflows in der Software-Entwicklung, die oft in global verteilten Teams erfolgt. Und auch unter Security-Gesichtspunkten ergäben sich klare Vorteile: Denn sind die einzelnen Funktionen auf einem Steuergerät klar getrennt, erhöht das den Schutz vor Angriffen von Cyber-Kriminellen. Selbst wenn es Hackern gelänge, sich Zugang zu einer Funktion zu verschaffen, bliebe der Weg in andere Funktionsbereiche der Fahrzeugsteuerung erschwert. Eine wenig reizvolle Aussicht für Kriminelle, die es auf größtmöglichen Schaden beim angegriffenen Automobilhersteller anlegen.

Entkopplung ist sinnvoll – aber wie?

Eine auf Autosar 4.x basierende Architektur definiert bereits grundlegende Mechanismen, um die unterschiedlichen Softwaremodule auf einem Steuergerät unabhängig voneinander zu entwickeln und bietet auch grundlegende Elemente, um diese gegeneinander abzugrenzen (beispielsweise Speicherschutz). Allerdings setzt die konsequente Umsetzung der in Autosar angedachten Konzepte eine spezifische Erweiterung voraus: Es bedarf eines Hypervisors, der das einzelne Steuergerät in unterschiedliche virtuelle Maschinen (VM) partitioniert. Ein solcher Ansatz verspricht, dass sich Updates und Upgrades einzelner Funktionen ohne Beeinträchtigung der anderen Funktionen auf dem Steuergerät durchführen lassen. Der Modifikation einzelner Funktionen müsste in diesem Fall also keine umfassende Re-Validierung sämtlicher Software auf dem Steuergerät vorausgehen.

Die Partitionierung sorgt dafür, dass sich die jeweilige Software in einem Zustand wähnt, in dem für jede Funktion eine eigene Hardware zur Verfügung steht. Die Funktionen sind dabei so strikt entkoppelt, dass sie bei Updates und Upgrades ohne komplette Re-Validierung einzeln modifiziert werden können. Und nicht nur das. Schon in der Entwicklung des Steuergeräts können die beteiligten Softwareunternehmen dank der Partitionierung völlig unabhängig voneinander arbeiten. Softwarefehler oder böswillige Eindringlinge bleiben lokal auf einzelne VMs begrenzt. Der Grad der Entkopplung ist so hoch, dass 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 betrieben

Eck-DATEN

Agile Software-Entwicklung schafft die Möglichkeit, softwaregesteuerte Fahrzeugfunktionen durch fortlaufende Updates und Upgrades auf den jeweils neuesten Stand zu bringen – auch im Feld. Um diese Updates ohne Sicherheitsrisiken aufspielen zu können, ist eine strikte Trennung der einzelnen Funktionen erforderlich. Dem entgegen steht der Trend der steigenden Vernetzung von immer mehr Funktionen auf zentralen Steuergeräten. Ein Weg diesen Widerspruch aufzulösen, ist die Partitionierung. Das war bisher jedoch mit den Mikrocontrollern in Automotive-Steuergeräten technisch nicht möglich. Der Lightweight Hypervisor von Etas löst die Probleme.

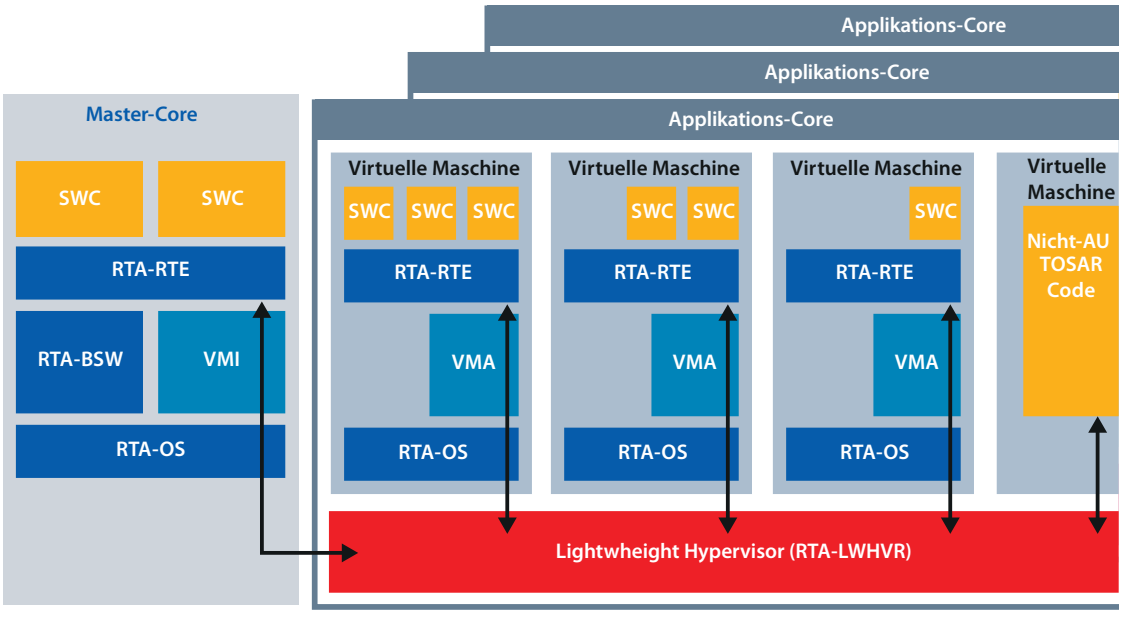


Bild 1: Schematischer Aufbau eines Steuergerätes mit dem Lightweight Hypervisor Etas RTA-LWHVR.

RTA-BSW AUTOSAR-Basissoftware
RTA-OS Betriebssystem
RTA-RTE Laufzeitumgebung
↔ Inter-Core-Kommunikation

SWC Softwarekomponente in gesicherter Anwendung
VMA Adapter zur virtuellen Maschine
VMI Virtuelle Maschinenschnittstelle

Bild 2: Zeitmanagement in einem Applikations-Core. Zusätzlich angeforderter Laufzeitbedarf wird in die freien Bereiche vom Hypervisor eingefügt.

werden kann – ohne dass dabei für das Gesamtsystem Beeinträchtigungen der Safety und Security drohen.

Für den Einsatz im Automobil optimiert

Prinzipiell kann der Hypervisor-Ansatz die nötigen Voraussetzungen für die agile Software-Entwicklung im Steuergerätebereich schaffen. Doch hierbei kommt es auf die Umsetzung an. Anpassungen an spezifische Anforderungen von Automotive-Steuergeräten sind unabdingbar. So benötigen Hypervisor im Normalfall ein eigenes Speichermanagement und ein Management der Zugriffsberechtigungen. Solch ein Hypervisor-Privilege-Modus hat in klassischer Ausführung drei Ebenen: den Hypervisor selbst, eine Basissoftware sowie die Applikationsfunktionen. Schon diese Anforderungen sprengen im Fahrzeugumfeld den Rahmen. Weder werden ein entsprechendes Speichermanagement vollumfänglich noch der dreistufige Hypervisor-Privilege-Modus von heute eingesetzten Fahrzeug-Mikrocontrollern unterstützt. Vor einem breiten Einsatz der Hypervisor-Technologie im Automobil gilt es, dieses Problem zu lösen.

Eben dies ist Etas nun mit dem Lightweight Hypervisor (RTA-LWHVR) für einen großen deutschen Fahrzeughersteller gelungen. Der für den Einsatz im Automobil optimierte Hypervisor hat dank einer neuartigen Architektur und flexibilisierter Kommunikationsstrukturen nur noch fünf Kilobyte (kB) Speicherbedarf sowie um Faktor vier bis fünf verkürzte Zugriffszeiten. Im konkreten Projekt wurde ein zentrales Body-Steuergerät in elf virtuelle Maschinen partitioniert, welche jeweils für Software von unterschiedlichen Zulieferern reserviert waren. Die ASIL-Einstufung reichte dabei von QM bis B.

Über Autosar hinaus

Trotz der Menge und Heterogenität der Softwarefunktionen verlief deren gekapselter Betrieb in dem Projekt problemlos. Möglich ist dies unter anderem, weil die Rechnerkerne beim Lightweight Hypervisor in einen Master-Core und diverse Applikations-Cores aufgeteilt sind. Die Trennung sorgt dafür, dass der Master-Core das Hardwaremanagement, den Betrieb der zentralisierten Basissoftware und einiger weniger Software-Applikationen übernimmt, während die Applikations-Cores einzig und allein die strikt getrennten virtuellen Maschinen beherbergen (Bild 1). Dabei besteht auch auf einem einzelnen Steuergerät die Wahl zwischen aufgeteilten Laufzeitumgebungen gemäß Autosar, mit einem Autosar Runtime Environment (RTE) oder nicht-Autosar-konformer Software.

Ein weiterer wichtiger Erfolgsfaktor: Die virtuellen Maschinen greifen zwar auf einen gemeinsamen Speicher zu; diese Zugriffe sind aber klar geregelt. Zusätzlich sind die Ausführungszeiten auf dem Kern klar definiert. Um schnelle Reaktionen zu ermöglichen, können Funktionen zusätzlich zu ihrer ohnehin garantierten Ausführungszeit weitere Zeitbudgets anfordern, ohne dass es dadurch zu Abstrichen bei der Ausführung anderer Funktionen kommt (Bild 2). Die Echtzeit-Anforderungen bleiben also jederzeit gewährleistet.

In der konkreten Umsetzung läuft dieser flexibilisierte Zugriff so, dass die virtuellen Maschinen im Fall eines deutlich erhöhten Laufzeitbedarfs beim Hypervisor anfragen können, ob sie über die für sie vorgesehene Kapazität hinaus vorübergehend auf zusätzliche Laufzeitkapazitäten zugreifen können. Der Lightweight Hypervisor priorisiert die Anforderungen und sorgt dafür, dass beim temporären Zugriff auf den Laufzeitpuffer keine andere Funktion beeinträchtigt wird.

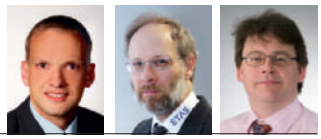
Marktreife Lösung für agile Software-Entwicklung

Weil es gelungen ist, den Speicherbedarf des Overheads auf 5 kB und den Leistungsbedarf auf nur fünf Prozent der verfügbaren Kernkapazität zu reduzieren, fügt sich der Lightweight Hypervisor problemlos in die technischen Randbedingungen für eingebettete Systeme im Automobil ein. Damit räumt er eine Hürde aus dem Weg, an welcher der breite Einsatz klassischer Hypervisor-Ansätze in Fahrzeugen bisher scheiterte. Sein schlanker Ressourcenbedarf schafft Flexibilität für den Einsatz in Steuergeräten unterschiedlichster Fahrzeugdomänen. Und er ist bereits für zahlreiche Mikrocontroller im Markt verfügbar.

Damit schafft die Lightweight-Hypervisor-Lösung die Voraussetzung für eine zuverlässige, leistungsfähige Partitionierung von Seriensteuergeräten, die den Weg zu sicheren Updates und Upgrades von Fahrzeugfunktionen ebnet. Hersteller von Steuergerätesoftware können in der Entwicklungsphase ebenso frei und unabhängig voneinander agieren, wie bei der Weiterentwicklung der softwaregesteuerten Funktionen nach dem Produktionsstart, welche dann in der Werkstatt oder Over-the-Air ins Fahrzeug kommen. Obendrein steigt das Sicherheitsniveau durch die Kapselung der Funktionen, obwohl auf den einzelnen Partitionen Software unterschiedlichster Sicherheitsklassen betrieben werden kann – ganz gleich, ob diese Autosar-konform ist oder nicht.

Diese Flexibilität wird nicht nur die Workflows in der Software-Entwicklung entzerrten, sondern gerade im Umfeld agiler Software- und Funktionsentwicklung zur spürbaren Senkung des Testaufwandes führen. Denn die intelligente Inter-Core-Kommunikation und strikte Kapselung erlauben es, Funktionen ohne aufwendige Re-Validierung des Gesamtsystems zu modifizieren. Damit ist eine zentrale Bedingung für sichere Funktions-Updates und -Upgrades an Fahrzeugen erfüllt.

Von dieser Möglichkeit werden Kunden in doppelter Hinsicht profitieren. Beim Kauf eines Fahrzeugs können sie künftig bedenkenlos eine günstige Basisversion auswählen und diese nach und nach mit Upgrades individualisieren. Und im laufenden Betrieb steigert die zuverlässige Partitionierung das Sicherheitsniveau unter anderem dadurch, dass Hersteller jederzeit bedarfsgerechte Sicherheitsupdates durchführen können – ohne Sorge, dadurch andere Funktionen zu beeinträchtigen. Gerade im Kampf gegen Cyber-Kriminelle und deren ständig neue Angriffsstrategien ist die Möglichkeit zur schnellen Umsetzung von Updates ein entscheidender Vorteil. *(ku)* ■



Autoren

Dr. Alexander Leonhardi
Senior Manager RTA Solutions und Consulting bei Etas

Dr. Gary Morgan
Senior Consultant bei Etas

Dr. James Dickie
Produktmanager für RTA-Produkte bei Etas

all-electronics.de
infoDIREKT 404ael1217