ISSN (Print) 1862-1791 | ISSN (Online) 2192-8878

Springer Vieweg

ATZ elektronik

03 März 2019 | 14. Jahrgang

FUNKTIONALE SICHERHEIT
Separation Kernel als Basis für zertifizierbare Systeme

© erdikocak | iStock

Separation Kernel – Basis für zertifizierbare Anwendungen und Systeme

Funktionale Sicherheit und Cyber Security zählen zu den wichtigsten Themen bei der Entwicklung komplex vernetzter Fahrzeugsysteme. Der Zertifizierung einzelner Systeme wird in Zukunft eine immer größere Bedeutung zukommen. Hier hat die Autoindustrie Nachholbedarf und kann von Zertifizierungslösungen aus der Luftfahrt lernen. Unter anderem gilt es, nach dem Prinzip „Safety and Security by Design“ zu arbeiten. Echtzeitbetriebssysteme auf Basis eines sogenannten Separation Kernel ermöglichen dabei neue Ansätze, wie Sysgo erklärt.

AUTOR

Chris Berg
ist Solution Architect Automotive bei der Sysgo AG in Klein-Winternheim.

HERAUSFORDERUNGEN

Schon heute sind viele Funktionen in Automobilen vollständig oder teilweise automatisiert; Fahrerassistenzsysteme wie Abstandswarner, Rückfahrkameras oder Einparkhilfen finden Zugang in die Serienproduktion selbst kleiner und mittlerer Fahrzeuge. Komplett autonom fahrende Pkw, Busse und auch Lkw sind auf öffentlichen Straßen im Testbetrieb; erste Serienfahrzeuge können sich zumindest teilautonom bewegen. Das Auto der Zukunft wird noch mehr Elektronik und Rechenleistung benötigen – einerseits, um die Sicherheit zu erhöhen (Fahrerassistenzsysteme) und andererseits, um den Anforderungen der Passagiere nach Komfort, Unterhaltung und Kommunikation zu entsprechen. Das Internet der Dinge, das Geräten innerhalb des Fahrzeugs die dafür notwendige Konnektivität verleiht, bringt dabei erhebliche neue Herausforderungen an die Sicherheit mit sich. Sicherheitsaspekte bestimmen daher zunehmend das Softwaredesign, und Zertifizierungsstandards werden im Automobilbau bald eine ähnlich wichtige Rolle spielen wie heute in der Flugzeugindustrie. Neben der funktionalen Sicherheit (Safety) treten dabei auch Aspekte der IT-Sicherheit (Security) und des Datenschutzes in den Vordergrund.

SAFETY UND SECURITY

Safety befasst sich mit der funktionalen Sicherheit und damit der Vermeidung von Systemausfällen, die zu Gesundheitsschäden und zu Beeinträchtigungen der Umwelt führen können. Mit der IEC 61508 gibt es hier eine branchenunabhängige Basisnorm für die funktionale Sicherheit elektrischer, elektronischer und programmierbarer Systeme mit Sicherheitsbezug. Die IEC 61508 unterscheidet vier Kritikalitätsstufen: SIL 4 bis 1 (Safety Integrity Level). Aufbauend auf dieser Norm definiert die ISO 26262 speziell die Anforderungen an die funktionale Sicherheit für Fahrzeuge im Straßenverkehr. Angelehnt an die Sicherheitsintegritätslevel der IEC 61508 und abhängig von der tolerierbaren Ausfallhäufigkeit definiert sie die vier Automotive Safety Integrity Levels (ASILs) D bis A, wobei D für die kritischsten Systeme steht, **BILD 1**.

Für die IT-Sicherheit geht es dabei vor allem darum, kritische Systeme vor unerlaubten Zugriffen und damit vor Manipulation, aber auch vor dem unbefugten Zugriff auf personenbezogene Daten zu schützen. In der Security gibt es ebenfalls internationale Standards für sicherheitskritische Systeme. Der weltweit wichtigste ist die ISO 15408, besser bekannt als Common Criteria (for Information Technology Security Evaluation) für die Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten. Er führt sieben Evaluation Assurance Levels (EAL 1 bis 7) für die Vertrauenswürdigkeit ein. Im Bereich der Automobilindustrie arbeitet SAE International (ehemals Society of Automotive Engineers) derzeit an einer Reihe von Standards zu unterschiedlichen Aspekten von IT-Systemen in Automobilen und führt dabei im Draft J3061, in 2016 veröffentlicht und an die SILs angelehnt, den Begriff Automotive Cyber Security Integrity Level (ACsIL) ein. In der ISO wird zudem an der ISO 21434 (Road Vehicles – Cybersecurity Engineering) gearbeitet. Es steht zu erwarten, dass nach Verabschiedung dieser Standards für viele Produkte auch eine entsprechende Zertifizierung erforderlich werden wird. Schon heute besitzen einige Produkte eine Zertifizierung nach Common Criteria (CC). Dies bedeutet jedoch nicht automatisch, dass sie deswegen sicher sind – es muss auf jeden Fall detailliert darauf geachtet werden, was hier genau zertifiziert wurde.

Safety und Security lassen sich am einfachsten gewährleisten, wenn sämtliche IT-Systeme strikt voneinander getrennt sind und sich daher nicht gegenseitig beeinflussen können. Doch heute werden in Fahrzeugen immer mehr sicherheitskritische und unkritische Anwendungen betrieben., Um Kosten und Gewicht zu sparen, dient eine Hardware als Plattform für unterschiedliche Funktionen auch verschiedener Kritikalitätsstufen. Dieser Trend birgt erhebliche Risiken. Erhält beispielsweise ein Angreifer Zugriff auf ein vergleichsweise unsicheres Entertainmentsystem auf Basis von Android, und kann er über dieses Einfallstor auch auf sicherheitskritische Systeme zugreifen, hat das unter Umständen gravierende Konsequenzen. Es ist daher unabdingbar, Anwendungen mit unterschiedlichen Kritikalitätslevels strikt voneinander zu trennen, auch wenn sie auf der gleichen Hardware laufen. Hier kann die Automobilindustrie von den Erfahrungen in der Luft- und Raumfahrt mit ihren extremen Anforderungen profitieren, in der sich bereits hypervisorbasierte Lösungen durchgesetzt haben.

Funktion	Gefahr	ASIL-A	ASIL-B	ASIL-C	ASIL-D
Fahren	Plötzlicher Start				
	Abrupte Beschleunigung				
	Verlust an Fahrleistung				
Bremsen	Maximale 4-Rad-Bremsung				
	Verlust an Bremsleistung				
Lenken	Eigenlenkung				
	Lenksperre				
	Assistenzverlust				

BILD 1 Je nach Funktion sind unterschiedliche ASILs erforderlich; D ist der stringenteste Level (© Sysgo)

MEHRERE PARTITIONEN STATT MULTIPLER CPUS

Ein Hypervisor kann auf einem Controller unterschiedliche Funktionen in mehreren Partitionen hosten, die bisher separate CPUs erforderten. Allerdings muss dabei sichergestellt werden, dass die Software, die die Hypervisorfunktionalität zur Verfügung stellt, tatsächlich eine strikte Trennung zwischen den Partitionen garantiert. Ansonsten hat man zwar eine einheitliche Hardwareplattform, aber möglicherweise Interaktionen zwischen kritischen und nicht-kritischen Anwendungen wie etwa Audiosystem und Bremsen. Eine Zertifizierung nach

ASIL-D und ISO 26262 gibt hier die Sicherheit, dass Funktionen in unterschiedlichen Partitionen tatsächlich so voneinander getrennt sind, als liefen sie auf unterschiedlichen CPUs.

Insbesondere auf Multicoresystemen ist der Einsatz von Hypervisoren grundsätzlich eine geeignete Möglichkeit, den Herausforderungen beim Systemdesign zu begegnen. Primär werden solche CPUs zwar aus Performancegründen verwendet, doch sie können auch die verlangte Trennung einzelner Funktionen unterstützen. Allerdings ist die Zertifizierung von Multicore-Systemen sehr komplex, und viele zertifizierte Systeme nutzen tatsächlich nur einen Kern. Werden allerdings unterschiedliche Funktionen in einer einzelnen Software gebündelt, die unter einem Echtzeitbetriebssystem (Real-time Operating System, RTOS) auf nur einem CPU-Kern läuft, können sehr leicht Interferenzen zwischen den Funktionen auftreten – die strikte Trennung ist nicht gewährleistet. Beispielsweise kann die Auswirkung einer Anwendung auf das Laufzeitverhalten einer anderen Anwendung zu Sicherheitsproblemen führen, etwa das Überschreiten von Fristen bei Echtzeitanwendungen. Auf ähnliche Weise können Timingeffekte aufgrund der gemeinsamen Nutzung der Systemressourcen – wie Caches und Speicherbusse – zu verborgenen Informationskanälen führen, die gegen die Vertraulichkeitsanforderungen der Anwendung verstoßen. Diese potenziellen Probleme rühren vor allem daher, dass die meisten Hypervisoren nachträglich einem RTOS zugefügt werden, das vom eigenen Design her eine solche Trennung nicht unterstützt. Gerade in sicherheitskritischen Anwendungen ist es aber wichtig, dass bereits das RTOS speziell für die getrennte Ausführung unterschiedlicher Funktionen ausgelegt ist, es also vom Design her eher ein Separation Kernel denn ein simples RTOS ist.

RÄUMLICHE UND ZEITLICHE TRENNUNG

Ein solcher Separation Kernel ermöglicht die räumliche und zeitliche Trennung zwischen Anwendungen und stellt die Partitionen für die Ausführung von Benutzeranwendungen bereit. Die zeitliche Trennung erfolgt dabei durch Zeitpartitionierung, bei der die CPU-Zeit während der Konfiguration in Zeitpartitionen aufgeteilt wird. Die räumliche Trennung erfolgt durch Ressourcenpartitionierung, bei der die Systemressourcen wie Hauptspeicher, Dateien, Geräte, sichere Kommunikationskanäle und Kerne partitioniert und Containern, den sogenannten Ressourcenpartitionen, statisch zugewiesen werden. Benutzeranwendungen werden dabei im Kontext einer Ressourcenpartition ausgeführt.

Ein Beispiel für eine Softwareumgebung mit strikter Trennung von Anwendungen ist PikeOS von Sysgo, das sich bereits in der Flugzeugindustrie bewährt hat. PikeOS bietet sowohl ein volles Echtzeitbetriebssystem (Hard RTOS) als auch ein Virtualisierungs- und Partitionierungssystem, um die besonderen Anforderungen von Anwendungen in der Automobilindustrie zu unterstützen, **BILD 2**. Die Basis der PikeOS-Plattform ist ein Micro Kernel, der eine Virtualisierungsinfrastruktur zur Verfügung stellt. Damit ist es möglich, verschiedene Anwendungen und Ressourcen in sicheren, individuellen Partitionen zu platzieren. Diese können in den verschiedensten Umgebungen laufen – von Posix über Linux und Android bis Autosar oder Genivi, **BILD 3**. Dank der integrierten Zeitpartitionierung ist es dabei unerheblich, ob es sich um Echtzeitapplikationen handelt oder nicht. Der Separation Kernel von PikeOS 4.2.2 ist derzeit weltweit der einzige, der eine Zertifizierung nach CC EAL 3+ besitzt (für die verbreiteten Plattformen X86_64, ARMv7 und ARMv8).

Insbesondere in gemischten Umgebungen mit relativ schlecht gesicherten

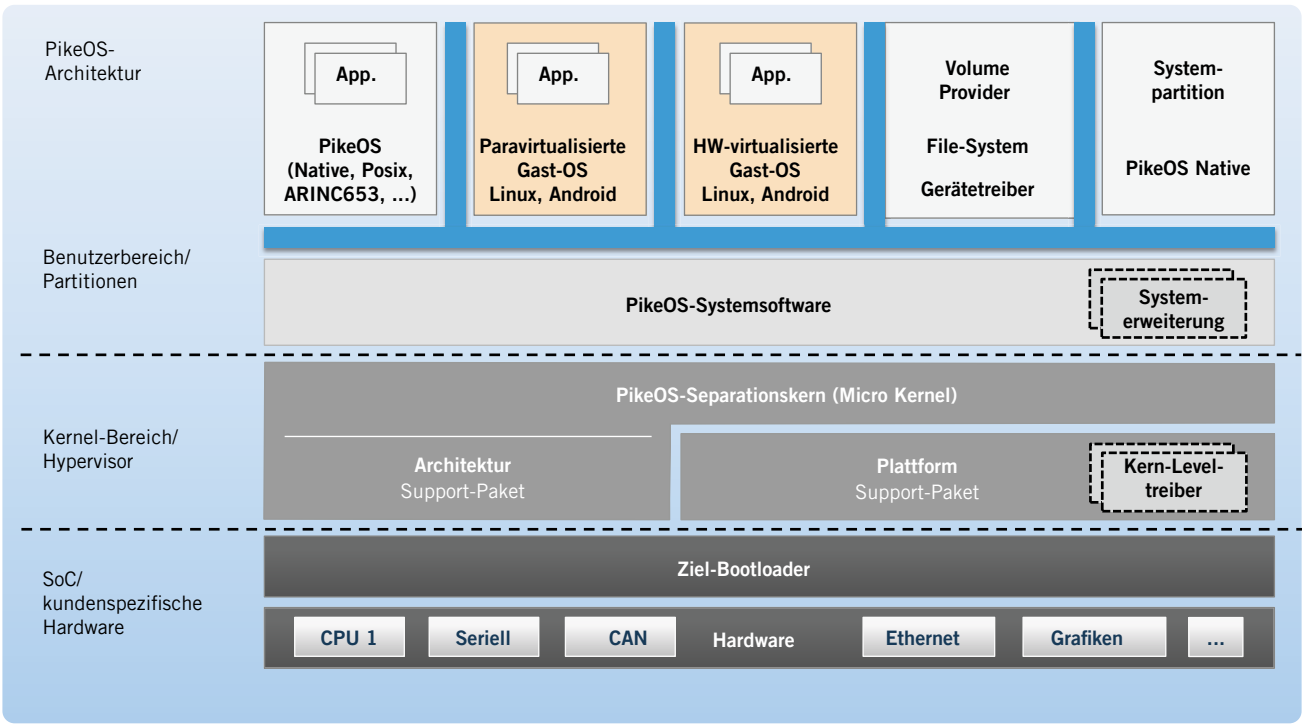

BILD 2 Der Separation Kernel von PikeOS sorgt für eine sichere Trennung der verschiedenen Partitionen (© Sysgo)

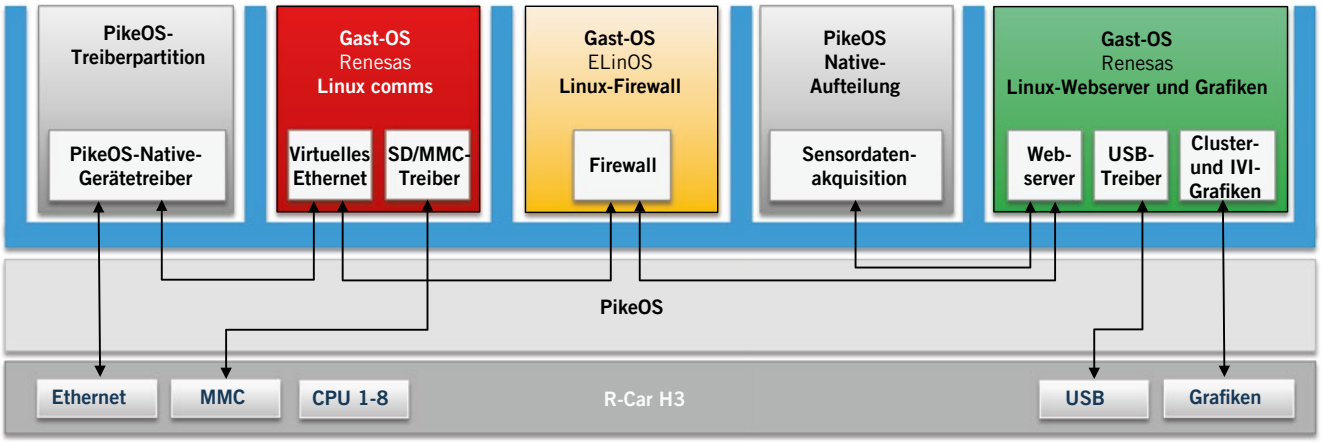

BILD 3 PikeOS in einer Automobilanwendung auf Basis des Renesas R-Car H3 (© Sysgo)

Betriebssystemen wie Android und kritischen Umgebungen wie Autosar kann ein Separation Kernel auch eine wichtige Sicherheitsfunktion erfüllen, um Angriffe zu erschweren. Dieser Kernel, der als Hypervisor für die unterschiedlichen Gastbetriebssysteme agiert, ist in der Lage, privilegierte Systemaufrufe der Gastsysteme abzufangen und zunächst auf die erforderlichen Berechtigungen zu prüfen, bevor sie tatsächlich ausgeführt werden. Während übliche Desktop-Betriebssysteme alle Gerätetreiber im Kernel integriert haben, kann man so eine Umgebung schaffen, in der nur ein sehr kleines Set von Diensten im „Privileged Mode“ im Kernel abläuft – etwa Scheduling, Context Switching, Prozesskommunikation sowie -synchronisation und Interrupt-Handling. Gerätetreiber werden dann ohne Privilegien im ganz normalen Anwendermodus ausgeführt wie jeder andere Anwendungscode. Auf diese Weise wird die Angriffsfläche des gesamten Systems deutlich reduziert.

SICHERHEIT UND ZERTIFIZIERUNG

Der PikeOS-Hypervisor selbst ist nach höchsten Industriestandards zertifiziert und damit eine geeignete Grundlage für kritische Systeme, in denen sowohl funktionale Sicherheit als auch IT-Sicherheit gewährleistet sein müssen. Die Schutzmechanismen basieren dabei im Wesentlichen auf zwei den Grundsätzen strikte Trennung der Anwendungen durch Zeit- und Ressourcenpartitionierung sowie Steuerung der Kommunikationskanäle. Die einzelnen Anwendungen innerhalb des Gesamtsystems können dabei unterschiedliche Kritikalitätslevel besitzen.

Aufgrund dieser Schutzmechanismen von PikeOS kann die Zertifizierung nach branchenspezifischen Safety- und Security-Standards für jede Anwendung separat durchgeführt werden – ein wesentliches Merkmal, um die Kosten unter Kontrolle zu halten. Zudem war PikeOS die erste Plattform, die auch eine SIL-4-Zertifizierung in Multicore-Umgebungen erhielt. Um die Anforderungen der ISO 26262 zu erfüllen, wird PikeOS optional mit einem „Automotive Certification Kit“ angeboten, in das die langjährige und umfassende Zertifizierungsexpertise von Sysgo eingeflossen ist. Der Zertifizierungsbausatz enthält einen ISO-26262-Teil-6-konformen PikeOS-Hypervisor sowie umfassende Dokumentationshilfen für Entwicklung und Test. Weiterhin können zusätzliche Sicherheitsinformationen bereitgestellt werden, um ISO-26262-konforme Systeme zu erreichen. Wichtige Bestandteile dieser Zertifizierungskits sind ein Sicherheitshandbuch mit Richtlinien für die Verwendung von PikeOS in sicherheitskritischen Designs von Systemen sowie eine Fallstudie mit charakteristischen Anforderungen der funktionalen Sicherheit entsprechend den jeweils notwendigen ASILs.