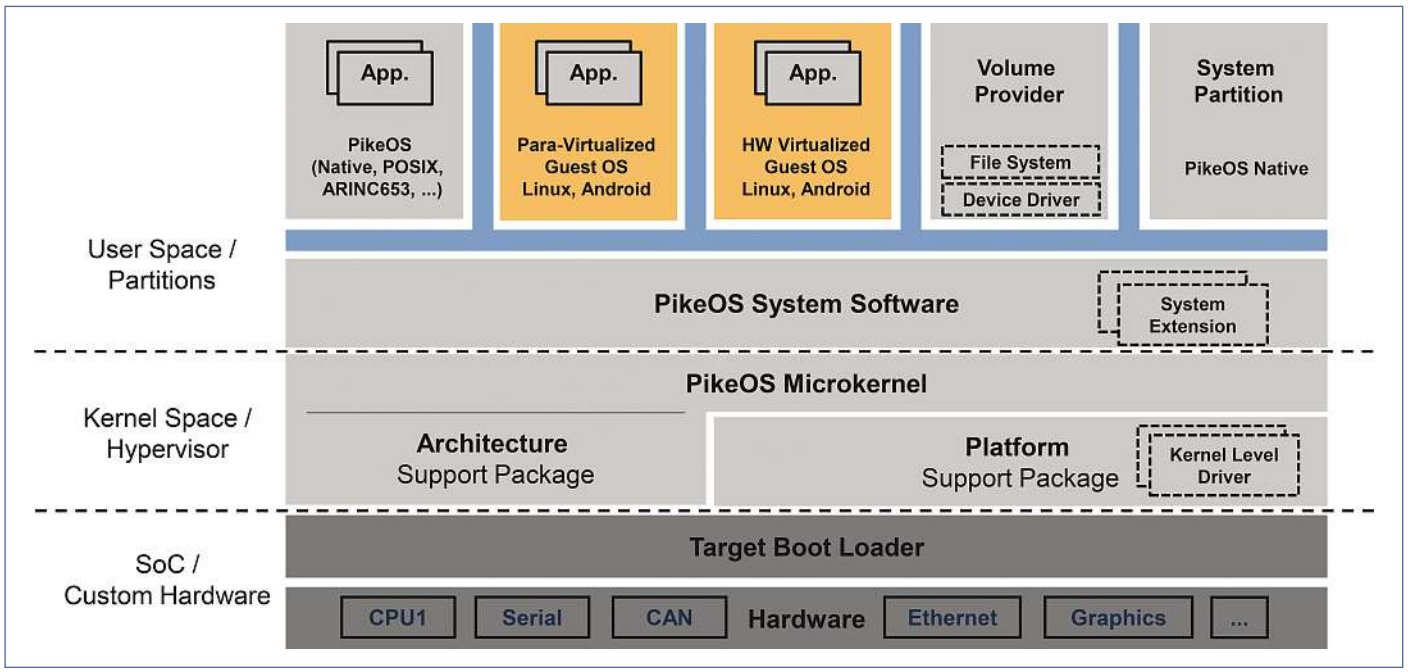

Bild: Sysgo AG

Bild 1: *Eine strikte Trennung von Anwendungen in Partitionen ist das grundlegende Designprinzip von PikeOS.*

Mehrere Anwendungen mit einem Separation Kernel konsolidieren

Immer mehr Anwendungen müssen auf immer weniger Hardware-Plattformen laufen. Der gemeinsame Betrieb sicherheitskritischer und unkritischer Anwendungen auf einer Plattform erfordert neue Ansätze.

MARKUS JASTROCH *

In vielen Bereichen, sei es Medizintechnik, Automotive oder fertigende Industrie, laufen viele Systeme noch parallel. Doch Konsolidierung mehrerer Anwendungen auf eine einzige Hardware-Plattform wird immer gefragter. Einer der Treiber der Konsolidierung, speziell in der Automobilindustrie und in der Luft- und Raumfahrt, ist die Gewichtsersparnis sowohl bei Systemen als auch bei der Verkabelung. Ein weiterer Faktor sind Stromaufnahme und Energiebedarf: Eine einzelne Hardware-Plattform ist ressourcenschonender und produziert weniger Abwärme als mehrere gleichzeitig laufende Systeme mit eigenen Prozessoren. Natürlich spielen in allen Industriebereichen natürlich auch die Kosten eine erhebliche Rolle. Eine geringere Vielzahl und Vielfalt an Hardwareplattformen reduziert sowohl Produktions- als auch Entwicklungskosten.

Bedenkt man, dass in einem normalen PKW heute ohne weiteres 60 bis 100 verschiedene CPUs bei marginaler Auslastung jeweils lediglich eine definierte Aufgabe erfüllen und über bis zu sieben Bussysteme miteinander kommunizieren, kann man das Potential der Konsolidierung mehrerer Systeme erahnen. Nicht anders ist es in vielen anderen Branchen, insbesondere dort, wo sicherheitskritische und unkritische Anwendungen parallel laufen müssen.

Trennung von kritischen und unkritischeren Systemen

Bei allen Problemen, die der Wildwuchs von CPUs mit sich bringt, hat er doch einen großen Vorteil: Er trennt die einzelnen Funktionen, so dass kein System von Fehlern in einem anderen beeinträchtigt werden kann, und sorgt so für ein hohes Maß an funktionaler Sicherheit. So kann in heutigen Fahrzeugen das Audiosystem keinesfalls auf die Bremsen einwirken, da beide von strikt getrennten Systemen kontrolliert werden.

Migriert man solch unterschiedliche Systeme auf eine einheitliche Hardware-Plattform, ist das nicht mehr von vornherein gewährleistet. Eine Trennung muss in diesem Fall also auf anderen Wegen erreicht werden. Im Zusammenhang mit der zunehmenden Vernetzung und insbesondere dem Internet of Things (IoT) treten dabei neben der funktionalen Sicherheit auch Aspekte der IT-Sicherheit und des Datenschutzes in den Vordergrund.

Bei der IT-Sicherheit geht es dabei vor allem darum, kritische Systeme vor unerlaub-

Markus Jastroch
... ist Director Marketing Communications bei der SYSGO AG in Frankfurt/Main.

ten Zugriffen zu schützen und damit vor Manipulation, speziell bei Automobilen und in der Medizintechnik auch vor dem unbefugten Zugriff auf personenbezogene Daten. Bei strikt getrennten Systemen, wie sie in der Vergangenheit üblich waren, ist das relativ einfach. Der Parallelbetrieb sicherheitskritischer und unkritischer Anwendungen auf einer Hardwareplattform birgt dagegen erhebliche Risiken. Erhält etwa ein Angreifer Zugriff auf ein vergleichsweise unsicheres Board-Entertainment-System, über das er als auf sicherheitskritische Systeme nutzen kann, hat das oft gravierende Konsequenzen. Es ist daher unabdingbar, Anwendungen mit unterschiedlichen Kritikalitäts-Levels strikt voneinander zu trennen, auch wenn sie auf der selben Hardware laufen.

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 absolut sichergestellt werden, dass die Software, die die Hypervisor-Funktionalität zur Verfügung stellt, tatsächlich eine strikte Trennung zwischen den Partitionen garantiert. Ansonsten hat man zwar eine einheitliche Hardware-Plattform, aber möglicherweise Interaktionen zwischen kritischen und nicht kritischen Anwendungen. Eine Zertifizierung gibt hier die Sicherheit, dass Funktionen in unterschiedlichen Partitionen tatsächlich so voneinander getrennt sind, als liefen sie auf unterschiedlichen CPUs. Dabei sind abhängig von der Branche unterschiedliche Standards einzuhalten, die jedoch in der Regel vergleichbare Anforderungen stellen.

Insbesondere auf Multicore-Systemen ist der Einsatz von Hypervisoren grundsätzlich eine geeignete Möglichkeit, den Herausforderungen beim System-Design zu begegnen. Primär werden solche CPUs zwar aus Performance-Gründen verwendet, doch sie können auch die verlangte Trennung einzelner Funktionen unterstützen.

Trennung von Anwendungen durch einen Separation Kernel

Der Einsatz von Hypervisoren allein ist aber keine Garantie für die strikte Trennung der unterschiedlichen Funktionen. Die meisten Hypervisoren werden auf ein Echtzeitbetriebssystem (RTOS; Real Time Operating System) aufgesetzt, 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 ist denn ein simples RTOS.

Die Verwendung unabhängiger Hardwarekomponenten für sicherheitsrelevante und andere Anwendungen sorgt für eine sichere Trennung, führt aber auch zu erhöhten Hardwarekosten. Ein auf einem Separation Kernel basierendes Betriebssystem wie etwa PikeOS von SYSGO ermöglicht dagegen die Trennung von Applikationscode auf derselben Hardwareplattform durch die Aufteilung der physikalischen und zeitlichen Ressourcen der Hardware.

Die Trennung von physikalischen Ressourcen wird als räumliche Trennung oder Ressourcenpartitionierung bezeichnet, während die Trennung der verfügbaren Ausführungszeit als zeitliche Trennung oder Zeitpartitionierung bekannt ist. Das Trennungsprinzip kann mit einem Hypervisor verglichen werden, doch der Hauptunterschied besteht darin, dass ein Separation Kernel die folgenden Fähigkeiten bietet:

- Unumgehbar: Eine Komponente kann den Kommunikationsweg nicht umgehen, auch nicht mit Lower-Level-Mechanismen.
- Manipulationssicher: Vermeidung von unbefugten Änderungen durch die Überwachung der Änderungsrechte für den Sicherheitsmonitor-Code, die Konfiguration und die Daten.
- Immer aktiv: Jeder Zugriff und jede Message wird von den entsprechenden Sicherheitsmonitoren überprüft.
- Evaluierbar: Vertrauenswürdige Komponenten können hinsichtlich der Sicherheit daraufhin evaluiert werden, ob sie modular, gut entworfen, gut spezifiziert, gut umgesetzt, klein, wenig komplex etc. sind.

In der Nomenklatur eines Separation Kernels werden isolierte Anwendungsbereiche als Partitionen bezeichnet. Die Trennung von Applikationen in Partitionen sorgt dafür, dass sich die Applikationen nicht gegenseitig stören, so dass jede Applikation auf ihrem zugeordneten Safety Integrity Level (SIL) arbeitet. So kann eine Hardwareplattform Anwendungen gemischter Kritikalitätsstufen verarbeiten. Ein Kommunikations-Stack (z. B. TCP/IP, Web-Server, OPC-UA...) kann in einer SIL 0-Partition gehostet werden, während eine sicherheitsrelevante Anwendung in einer SIL 4-Partition läuft. Jeder Partitionsinhalt muss in einem solchen Fall für seine jeweilige SIL-Ebene zertifiziert werden.

Hypervisor und Echtzeitbetriebssystem

PikeOS basiert auf einem Mikrokernel mit der Leistung eines traditionellen Echtzeitbetriebssystems. Der Hypervisor stellt Partitionen zur Verfügung, die verschiedene Anwendungen hosten können - von einer einfachen, aber hochkritischen Steuerungsaufgabe bis hin zu einem vollwertigen Betriebssystem wie Linux oder Android. Dies hat zur Folge, dass sichere und unsichere Anwendungen auf derselben Plattform koexistieren können. Komplexe Systeme, die in der Vergangenheit aus mehreren Geräten bestanden, können so auf einer einzigen Hardwareplattform konsolidiert werden. Der PikeOS Hypervisor läuft sowohl auf x86 als auch auf ARM, PowerPC, SPARC V8/LEON oder MIPS und kann problemlos an andere CPU-Architekturen angepasst werden.

PikeOS wurde speziell für die Entwicklung von Software in eingebetteten Systemen mit hohen Sicherheitsanforderungen entwickelt. Mit Echtzeit-Virtualisierung und Partitionierung bietet es alle Funktionen, die für die Entwicklung moderner multifunktionaler und hochintegrierter Geräte erforderlich sind. Die Software-Architektur bildet dabei auch die Grundlage für die Zertifizierung und behördliche Abnahme kritischer Systeme nach den Standards für funktionale Sicherheit und IT-Sicherheit, wie sie z.B. in der Luftfahrt und im Bahnwesen sowie häufig auch bei industriellen und medizinischen Anwendungen erforderlich ist. Die zunehmende Zahl von Softwareanwendungen und Assistenzsystemen im Auto wird auch hier einen deutlichen Trend zu Zertifizierungsanforderungen mit sich bringen.

Da es selbst nach den höchsten Industriestandards zertifiziert ist, stellt PikeOS eine gute Grundlage für kritische Systeme dar, die sowohl funktionale Sicherheit als auch IT-Sicherheitsanforderungen erfüllen müssen. Die Schutzmechanismen beruhen im Wesentlichen auf zwei Prinzipien: strikte Trennung der Anwendungen durch Zeit- und Ressourcen-Partitionierung sowie strikte Kontrolle der Kommunikationskanäle. Die einzelnen Anwendungen, aus denen sich das Gesamtsystem zusammensetzt, können unterschiedliche Kritikalitätsstufen repräsentieren.

Durch die von PikeOS bereitgestellten Schutzmechanismen kann die Zertifizierung nach branchenspezifischen Sicherheits- und/oder Sicherheitsstandards für jede Anwendung separat erfolgen - ein wesentliches Merkmal, um die Kosten unter Kontrolle zu halten, zumal die Kosten für die Zertifizierung ohne weiteres die Hälfte der gesamten Entwicklungskosten eines kritischen Systems ausmachen können. // SG

SYSGO