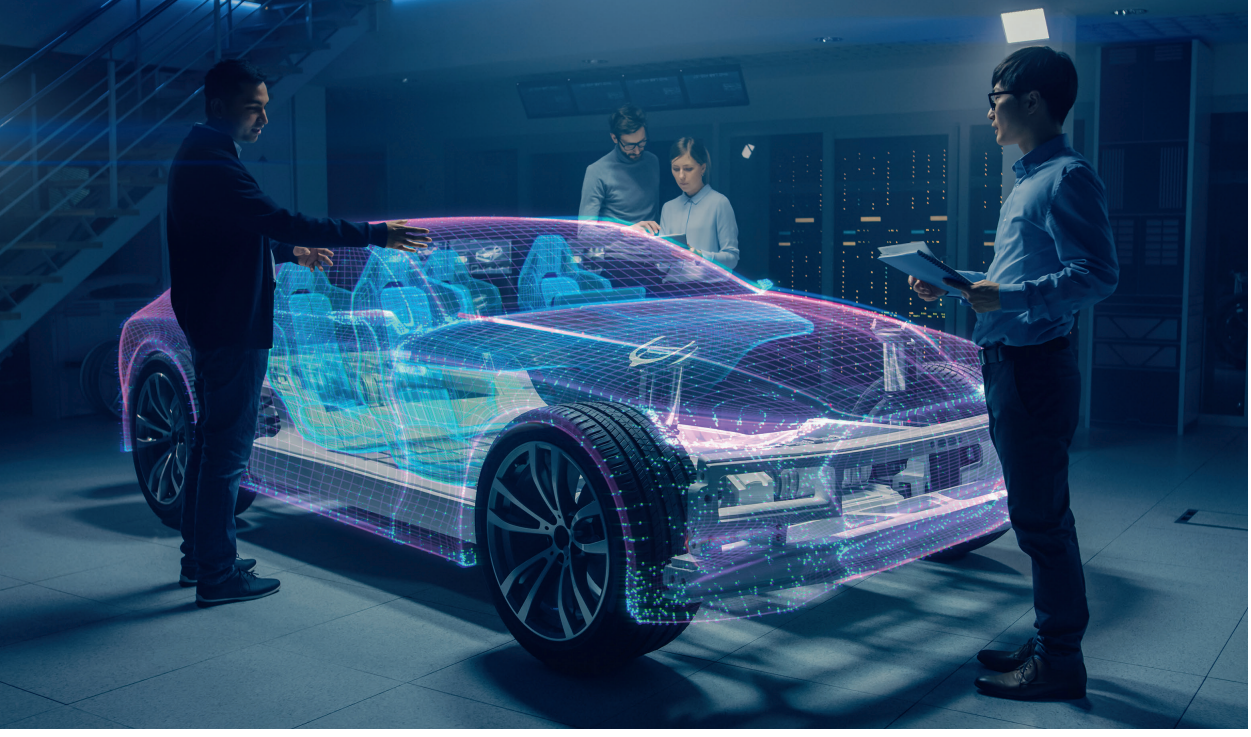

© Gorodenkoff Productions - Adobestock

Speichertechnologie

Funktionale Sicherheit inklusive Cybersicherheit

Die Architektur von Fahrzeugen ist im Wandel. Neue Funktionen der Automatisierung, Vernetzung und Personalisierung werden zunehmend durch Software realisiert. Doch Software-definierte Fahrzeuge bringen neue Risiken. Geeignete Lösungen zur Datenspeicherung können dazu beitragen, diese zu beherrschen.

Matthias Poppel

Wenn es früher um Sicherheitsfragen in der Fahrzeugentwicklung ging, war klar, dass man von funktionaler Sicherheit (englisch: safety) sprach. Mittlerweile haben sich Fahrzeuge zu kleinen Rechenzentren entwickelt, die dazu mit hoher Geschwindigkeit unterwegs sind. Die Folge: Mit jeder neuen digitalen Assistenz-, Infotainment- oder Servicefunktion steigen die Anforderungen an die Datensicherheit: Cyber Security, also der Schutz vor Datenmanipulation und -ausspähung, ist für Automobilbauer zu einem ernst zu nehmenden Thema geworden. Versäumnisse bei der Cybersicherheit wirken sich unter Umständen auf die funktionale Sicherheit aus. Es läge nahe, geschlossene, unveränderliche Systeme zu implementieren. Doch die Natur von Software-Defined-Systemen ist es, aktualisierbar und erweiterbar zu sein.

Die Hardware eines neuen Fahrzeugs ist fix, doch die Software muss ständig an neue Funktionen und Sicherheitsanforderungen angepasst werden können. Dabei geht es nicht nur darum, dass zum Beispiel viele Autofahrer eine vollständige Integration des Fahrzeugs in ihre digitale Welt erwarten. Es gibt konkrete Vorschriften, die eine disruptive Wirkung für die Hersteller haben: So verlangt beispielsweise die Cyber-Security-Regulierung der UNECE WP.29, dass neu entwickelte Fahrzeuge bereits heute über eine sichere Update-Möglichkeit verfügen müssen. Bei UNECE handelt es sich um das Harmonisierungsgremium der Vereinten Nationen, unter anderem zuständig für Fahrzeug-Typgenehmigungen in Europa.

Software-definierten Fahrzeugen gehört die Zukunft

Die Vorteile liegen auf der Hand: Funktionen werden in Zukunft individuell und nach Bedarf freigeschaltet – sogar als zeitlich limitierte Dienste, weil Software-Updates neue Vertrags- und Abrechnungsmodelle ermöglichen. Kommunizieren Fahrzeuge mit ihrer Umgebung und sammeln sie Daten im Realbetrieb, können diese Informationen zur Verbesserung von Diensten beitragen, die dem Fahrzeug dann über Over-the-Air-Updates zuteilwerden.

Eine in Smart-Grids eingebundene E-Mobilität, Car-Sharing, automatisiertes Fahren oder wie auch immer die nächsten Entwicklungen aussehen: Sie werden durch Software ermöglicht und können auch nach dem Kauf eines

Autos noch aktiviert werden. Über Updates kann so der Fahrzeugwert über den Lebenszyklus mit neuen Features gesteigert werden – fast wie beim Smartphone. Die Voraussetzung: Software und Hardware müssen entkoppelt sein, um die Wartungsfreundlichkeit über den gesamten Lebenszyklus eines Fahrzeugs zu garantieren: von der Inbetriebnahme bis zur Außerbetriebsetzung und dazwischen. Dies erfordert Produktarchitekturen, die eine sichere Over-The-Air-(OTA)-Update-Fähigkeit der Anwendungssoftware unterstützen.

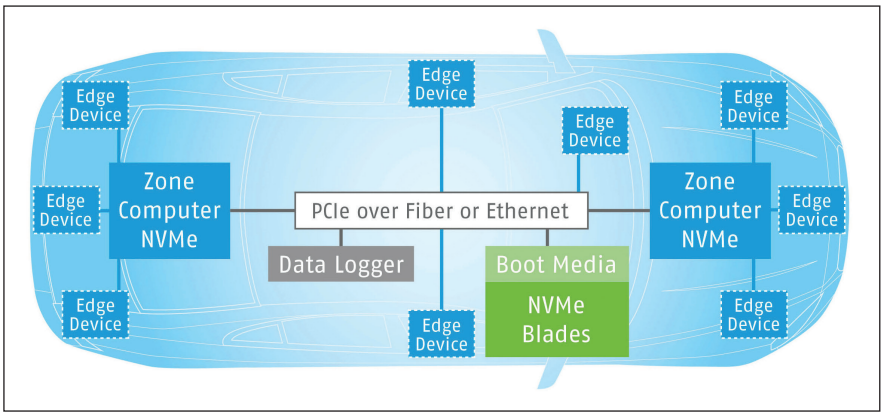

Bild 1: Zentralisierte Speicherarchitektur für zukünftige Automobilplattformen. © Swissbit

Neue Architektur-Anforderungen

Neue Hochleistungsanwendungen wie erweiterte Fahrerassistenzsysteme und autonomes Fahren (ADAS/AV), Infotainment, Drive Video/Data Recorder oder Instrumenten-Cluster erhöhen den Bedarf an skalierbarer Rechenleistung, was eine hohe Bandbreite und geringe Latenz bei der Speicherung erfordert. OEMs und Tier-1-Anbieter stehen damit vor der Herausforderung, leistungsfähige Rechensysteme zu entwickeln. Es dürfte sich anbieten, mit verschiedenen und untereinander kommunizierenden, aber voneinander getrennten zentralen Einheiten zu arbeiten. Hinzu kommen spezielle Sensor-Einheiten, die nach dem Prinzip des Edge-Computings funktionieren (**Bild 1**). Es braucht zonale Gateways beziehungsweise Domänensteuereinheiten mit Gateway-Funktionalität sowie Schnittstellen für PCIe, Ethernet und CAN oder LIN für die Sensorik. All diese brauchen Speichermodule mit höchster Zuverlässigkeit.

Keine funktionale Sicherheit ohne Cyber Security

Funktionale Sicherheit im Sinne der ISO 26262 erfordert den Nachweis wirksamer Mechanismen zur Minderung von Cyber-Security-Risiken, die beispielsweise in der ISO 21434 definiert sind. Diese beiden Normen gehen Hand in Hand, da ein direkter oder indirekter Cyber-Angriff sicherheitskritische Systeme beeinträchtigen kann. Unter Fachleuten ist unstrittig, dass rein Software-basierte Sicherheitseinrichtungen korrumpierbar sind. Daher brauchen Elektronikentwickler Hardware-basierte Sicherheitslösungen, um Daten und Geräte zu schützen und regulatorische Standards bis hin zu ASIL D einhalten zu können.

In anderen Anwendungsbereichen hat sich ein Ansatz bewährt, der auch beim Software-definierten Auto vielversprechend ist. Seit Jahren werden bereits Sicherheitsfunktionen in industrielle Flash-Speicher-Module integriert, um abhörsichere Handys, polizeiliche Bodycams und Kassensysteme abzusichern. Mit einem Sicherheitschip als Hardware-Anker und Verschlüsselungsfunktionen in der Firmware können sogar auswechselbare Memory-Cards die Funktion von TPM (Trusted Platform Module) oder anderen Hardware-Sicherheitsmodulen übernehmen.

Dazu gehören Secure-Boot, die Verschlüsselung von personenbezogenen Daten kundenindividueller Funktionen, der Schutz von geistigem Eigentum und natürlich die Verhinderung von Datenmanipulation. Sehr wichtig im Zusammenhang mit der Kommunikation der Subsysteme untereinander und der OTA-Updates ist die eindeutige Identifizierbarkeit von Kommunikationsteilnehmern. M2M-Kommunikationsteilnehmer erhalten gewissermaßen einen „fälschungssicheren Ausweis". So verhindern Authentisierungsmechanismen missbräuchliche Zugriffe auf Funktionen und Systeme eines Software-definierten Autos wirksam.

Vorsicht mit dem Flash-Speicher

SSDs und Memory-Karten aus dem IT- oder gar Consumer-Bereich sind für automobile Anwendungen ungeeignet. Aktuelle 3D-NAND-Chips sind nur auf höheres Datenvolumen hin optimiert, was aber mit kürzerer Lebensdauer und hoher Temperaturempfindlichkeit erkauft wurde. Die Entwickler von Automobilanwendungen brauchen Produkte, die auf Basis ausgewählter Chips industrietaugliche Speichermodule verwenden. Dies bezieht sich zunächst auf die Fertigung robuster Hardware, die beispielsweise AEC-Q100-zertifiziert ist oder in IATF-16949-zertifizierten Fabriken hergestellt wird.

Ganz entscheidend ist auch die Firmware der Speichermodule. Sie gleicht durch geeignete Mechanismen die fundamentalen Schwächen von NAND-Chips der TLC-Technologie aus und sorgt für weniger Empfindlichkeit gegenüber extremen Temperaturen. Auch Lebenszeiten und Datenerhalt können verlängert werden. Die Maßnahmen zum Ausgleich der technologisch bedingten Schwächen können bis hin zum pseudo-SLC-Modus reichen, der nur das starke Bit einer NAND-Zelle nutzt.

Fazit

Datenschutz- und Datensicherheitsaspekte werden bei neuen technischen Errungenschaften häufig zu spät beachtet, wie es immer wieder bei ungeschützten IoT-Geräten zu finden ist. Das in der Fahrzeugentwicklung fest integrierte Safety-Engineering wird dafür sorgen, dass dies nicht passiert und auch die Security-Thematik berücksichtigt wird. Hardware-basierte Sicherheit, integriert in Speichermodulen, kann dafür ein wichtiger Baustein sein. ■ (hh)

www.swissbit.com

Halle 1, Stand 534

Matthias Poppel ist Chief Sales & Marketing Officer bei Swissbit.
© Swissbit