Verlässliche Adaptive Software-Architekturen im Auto

Von Fail-Silent zu Fail-Operational

Software, Software-Architekturen, Zuverlässigkeit, Fail-Operational, Autonomes Fahren

Durch die zunehmende Automatisierung bis hin zum autonomen Fahren verändern sich auch die elektrisch-elektronischen (E/E) Architekturen sowie die Anforderungen an die Funktionalität von Fahrzeugen. Das hat zur Folge, dass Software-Architekturen eine zunehmende Flexibilität aufweisen und gleichzeitig eine erhöhte Zuverlässigkeit garantieren müssen.

Gereon Weiß

Der Automobilverkehr durchlebt derzeit einen radikalen Wandel: Der Fokus verlagert sich weg vom einzelnen Transportmittel hin zu flexibler Mobilität – sogar über das einzelne Fahrzeug hinaus. Diesen Paradigmenwechsel spiegeln auch die aufkommenden Trends am Automobilmarkt [1] wider:

Die sich ausbreitende Elektromobilität erfordert eine Veränderung und Vereinfachung der Fahrzeugarchitektur. So entfallen ohne Verbrennungsmotor mechanische Teile oder werden durch elektronische ersetzt. Das hat enormen Einfluss auf die notwendige Verlässlichkeit der eingesetzten IT- und Kommunikationssysteme [2].

Anhand der zahlreichen Ankündigungen der Fahrzeughersteller wird deutlich, dass auch die Automatisierung mit großen Schritten voran schreitet – bis hin zum autonomen Fahren. Dabei erstreckt sich die Entwicklung über verschiedene Stufen, die der Verband der Automobilingenieure SAE International folgendermaßen definiert [3]:

In Stufe 0 führt der Fahrer noch alle Steuerungsaufgaben selbst aus, in Stufe 1 assistiert bereits ein Fahrzeugsystem. Teilautomatisiert (Stufe 2) bedeutet, dass das System in bestimmten Anwendungsfällen Steuerungsaufgaben übernimmt. In Stufe 3 beginnt die Hochautomatisierung, das heißt der Fahrer muss das System nicht mehr dauerhaft überwachen, aber jederzeit in der Lage sein, die Kontrolle über das Fahrzeug zu übernehmen. Über Stufe 4 (vollautomatisiert) führt dann der Weg zum fahrerlosen Roboterauto der Stufe 5.

Darüber hinaus sind Fahrzeuge schon heute mit dem Backend bzw. der Cloud und zukünftig auch untereinander und mit der Infrastruktur vernetzt. Dadurch erzeugen sie eine hohe Vernetzung, oder sogenannte *Connectivity*. Und schließlich sorgen Ansätze neuer Mobilitätsnutzung für eine weitere Differenzierung des Automobilverkehrs. Zum Beispiel die Nutzung über einzelne Verkehrsmittel hinweg, Mobilitätsdienstleistungen oder Shared Mobility Konzepte.

Neue Technologien ermöglichen Disruption

Diese Trends führen dazu, dass Entwickler vollständig neuer Fahrzeuge höhere Freiheitsgrade genießen, als sie etablierten Fahrzeugherstellern offenstehen. So können beispielsweise neue Mobilitätskonzepte mit Kleinserienfahrzeugen etabliert werden, wie das Beispiel *Adaptive City Mobility* (ACM) [4] zeigt. In diesem Projekt wird eine flexible Fahrzeugnutzung von E-Fahrzeugen untersucht, sodass diese zum Beispiel sowohl als E-Taxi als auch als Transport- oder Leihfahrzeug genutzt werden können. Diese Anpassungsfähigkeit erfordert unter anderem eine flexible E/E-Architektur des Fahrzeugs sowie einfache Verfahren zum Batteriewechsel (*Bild 1*).

Anhand solcher Beispiele wird bereits ersichtlich, welche Potenziale sich aktuell durch die rasanten Technologieentwicklungen im IT-Bereich für die E/E Architekturen von Fahrzeugen ergeben. Darunter fallen besonders folgende Punkte [5]:

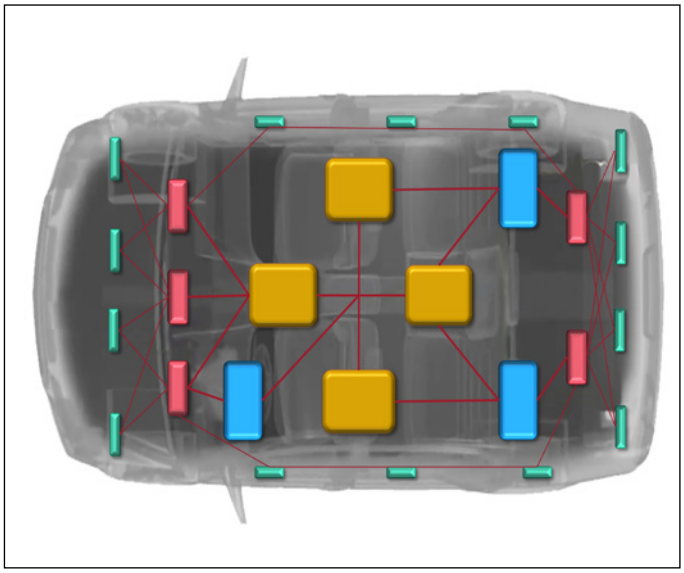
- Eine erhöhte Rechenleistung und Fortschritte im Bereich Künstliche Intelligenz schaffen die Voraussetzung für neue Automatisierungsgrade des Fahrens.
- Zentralisierte Rechenplattformen sorgen für eine Entkopplung der Sensorinformation von einzelnen Steuergeräten. Darüber hinaus stellen sie eine flexible Skalierbarkeit für verschiedene Fahrzeugausstattungen (low bis premium) und -generationen bereit (*Bild 2*).
- Hoch-performante Integrationsplattformen ermöglichen eine deutlichere Hierarchisierung und Optimierung der E/E-Architektur auf Gesamt-Fahrzeugebene.
- Der Wandel von einzelnen Funktionen hin zu dienstorientierten Software-Architekturen in Embedded Systems erlaubt es, die komplexer werdenden Interaktionen und Kombinationen der Funktionen zu handhaben.

Diese Änderungen sind auch bereits in AUTOSAR erkennbar, dem Standard für die Entwicklung von Software und eingebetteten Steuergeräten im Fahrzeug. Neben der bisherigen *Classic Platform* wird an der Standardisierung einer *Adaptive Platform* [6] gearbeitet, die erhöhte Rechenleistung für höhere Automatisierungsgrade bereitstellt. Im Weiteren müssen insbesondere auch die Interaktion mit Classic, Non-AUTOSAR Plattformen und die Vernetzung mit Backend bzw. Cloud betrachtet werden.

Verlässliche Automatisierung

Die Freiheitsgrade in der Entwicklung sowie die neuen technologischen Potenziale bergen natürlich die Herausforderung, dass auch die Anforderungen von Automotive-Systemen berücksichtigt werden müssen. Das wird besonders deutlich beim automatisierten Fahren. Dieses steht derzeit an der Schwelle der Entwicklung von einer Teil- zur Hochautomatisierung. Damit verbunden sind steigende Anforderungen an die Fahrzeugentwicklung. Das beinhaltet unter anderem die Verbesserung der Situationserkennung unter Verwendung hochgenauer

▲ Bild 1: Adaptive City Mobility – Fahrzeug mit Batteriewechselkonzept



▶ Bild 2: Schema einer zentralisierten und hierarchischen E/E-Architektur

digitaler Karten, eine Fahrstrategieplanung mit Unterstützung durch Künstliche Intelligenz sowie neue Methoden zur Absicherung der geradezu „explodierenden" Anzahl zu berücksichtigender Fahrsituationen.

Das Wichtigste aber ist: Der Mensch scheidet mit höheren Automatisierungsgraden zunehmend als Rückfallebene aus – und dies ab Stufe 5 des automatisierten Fahrens in allen Situationen. Besonders im Fehlerfall erfordert dies ein verändertes Verhalten des Fahrzeugsystems, das in der Lage sein muss, auch bei Fehlern selbst die Kontrolle zu behalten. Es ist daher nicht mehr ausreichend, wie es bisher gängige Praxis war, einzelne Systeme abzuschalten (sogenanntes *Fail-Silent-Verhalten*). Kritische Funktionen wie die Fahrzeugsteuerung müssen auch im Fehlerfall weiter funktionieren, bis ein sicherer Zustand erreicht werden kann (Fail-Operational-Verhalten).

Dies erfordert neue Konzepte, die vor allem auch die Software- und E/E Architektur im Allgemeinen betreffen. Der aktuelle Entwicklungsstand lässt kein sicheres vollautonomes Fahren zu. So vielversprechend Ansätze aus dem Bereich Künstlicher Intelligenz oder Machine Learning für die Automatisierung auch sein mögen, die Verlässlichkeit und Nachvollziehbarkeit der Verfahren reichen aktuell für sicherheitskritische Systeme [7] wie eine Fahrzeugsteuerung nicht aus.

Wichtig ist es daher, eine oder mehrere sichere Rückfallebenen im Fahrzeugsystem zu haben, die sicheres Verhalten auch im Fehlerfall garantieren. Für kritische Funktionen muss im Fehlerfall das sogenannte *Fault Tolerant Time Interval* (FFTI) eingehalten werden, um wieder einen sicheren Zustand herzustellen. Das FTTI beschreibt die minimale Zeit, die vergeht, bis eine potenzielle Gefahr nach einem Fehler auftreten kann. Ein Beispiel ist die maximal mögliche Ausfallzeit der Lenkfunktion, ohne dass das Fahrzeug unkontrollierbar erscheint.

Kann das System aus sich heraus nicht wieder den sicheren Zustand erreichen, muss in einen *Emergency Operation* Modus gewechselt werden (vgl. *Bild 3*). Dieser Modus kann schließlich doch noch ein sicheren Zustand herstellen. Dies kann beispielsweise durch den Wechsel in einen Notfallmodus mit reduziertem Funktionsumfang geschehen (z.B. minimalen Fahrzeugsteuerungsfunktionen).

Jedoch muss ein solcher Wechsel und der zugrunde liegende Adaptionsmechanismus auch die Anforderungen der sicherheitskritischen Funktionen berücksichtigen und immer verlässlich in einen sicheren Zustand führen. Die Implementierung einer solchen kontrollierten Adaption auf Fahrzeug-Systemebene erlaubt zudem eine erhöhte, kostengünstige Software-Redundanz und Flexibilität. So können je nach verfügbaren Ressourcen auch unterschiedliche Betriebsmodi oder Qualitätsstufen realisiert werden (*Graceful Degradation*).

Verlässlichkeit durch gezielte Redundanz

Um eine ausreichende Verlässlichkeit zu erzielen, muss eine grundlegende Redundanz des Systems vorhanden sein, wie beispielsweise eine von einzelnen Steuergeräten entkoppelte Sensorik/Aktuatorik, zweikanalige Kommunikation oder verlässliche Stromquellen. Basierend darauf kann mit ausreichenden Diagnosemechanismen der betroffenen Rechenplattformen bzw. Electronic Control Units (ECU) ein softwarebasierter

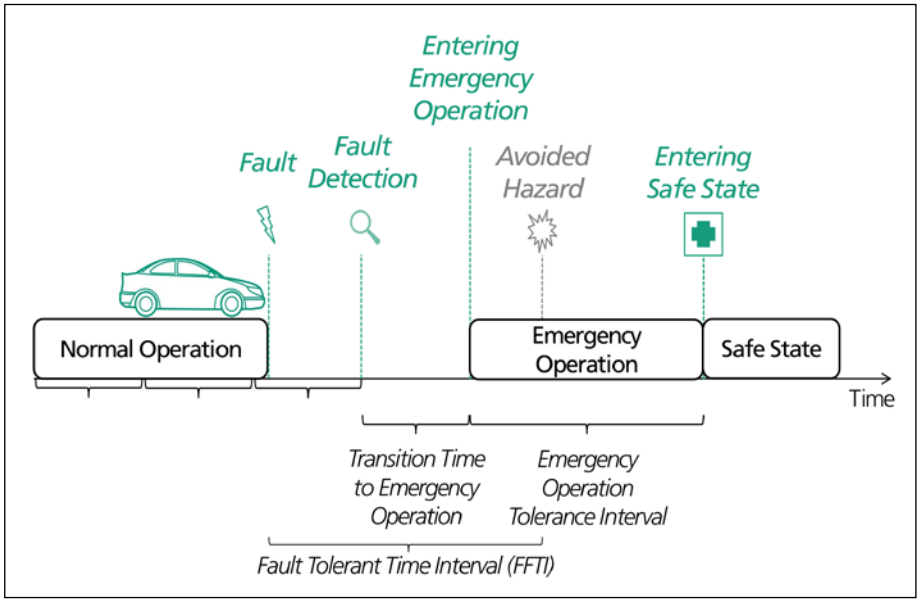


Bild 3: Fault-Tolerant Time Interval and Emergency Operation

Adaptionsmechanismus umgesetzt werden, der eine allgemeine Fehlerbehandlung ermöglicht [8]. Ein Vorteil für eine kosteneffiziente Systemauslegung ist hierbei, dass aufgrund des unterschiedlichen kritischen Potenzials nicht alle Funktionen gleich hohe Anforderungen wie gesteigerte Ausfallsicherheit erfüllen müssen. Das heißt: Nicht alle Funktionen müssen durch mehrfache Redundanz abgesichert werden.

Für ein solches *Mixed-Criticality System* ist eine effiziente Planung auf Systemebene notwendig, da die Menge möglicher Konfigurationen schon bei geringer Anzahl betrachteter Fehler und Funktionen stark anwachsen kann. Eine Lösung dieses Problems bietet die Nutzung eines *Safe Adaptation Cores*, wie er von Fraunhofer ESK mit entwickelt wurde [9]. Dieser stellt eine softwarebasierten Kontrollinstanz für die Erkennung und Behandlung von Fehlern in Echtzeit dar. Bei der Nutzung dieses Adaptionsmechanismus kann eine solche Planung automatisiert im Systementwurf erfolgen [10]. Dieser Ansatz lässt sich in verschiedenen Betriebsumgebungen nutzen, um eine verlässliche und adaptive Software-Architektur zu realisieren. So wurde er unter anderem erfolgreich in der Praxis eingesetzt, um automatisiert AUTOSAR-konforme Systeme zu entwickeln – durchgängig von der Planung bis zur automatischen Generierung von fail-operational Konfigurationen.

Neben AUTOSAR-basierten Systemen wurde der Ansatz durch Driver-in-the-Loop-Simulationen untersucht. Dabei wurden zu Testzwecken Fahrsituationen unter Beteiligung eines Fahrers nachgestellt. Diese Simulationen lieferten etwa Erkenntnisse darüber, wie viel Zeit zur Kompensation eines Fehlers vergehen kann: beim Ausfall der Lenkfunktion beispielsweise die Zeit, bis der Fahrer diesen bemerkt, ohne die Kontrolle über das Auto zu verlieren. Darüber hinaus wurde der Safe Adaptation Core-Ansatz in einem realen Elektrofahrzeug mit einer ausfallsicheren Steer-by-Wire-Lenkung sowie heterogenen Hardware-Plattformen und Software-Umgebungen erfolgreich überprüft [11]. Die Ergebnisse zeigen die Vorteile der vorgestellten software-basierten Adaption auf Systemebene. Im Vergleich zu einem mit dem Stand der Technik entwickelten ausfallsicheren System werden Potenziale hinsichtlich Kosten, Gewicht, Größe oder Energie deutlich (siehe *Bild 4*).

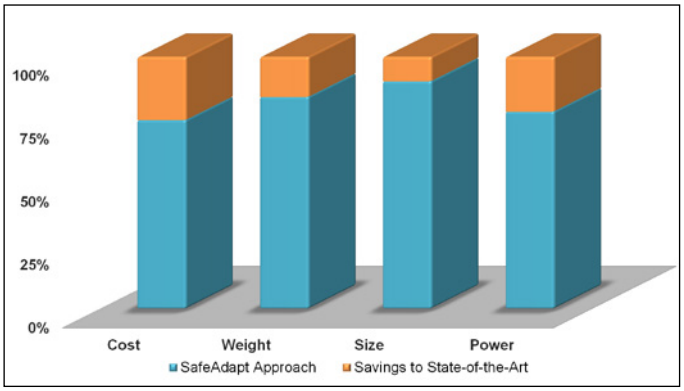


Bild 4: Vergleich Stand der Technik und Safe Adaptation Ansatz

Ausblick

Ab wann nun solche intelligenten Fail-Operational-Konzepte auch in Serienfahrzeugen Einzug halten, wird vorrangig von der Durchdringung hochautomatisierter Fahrfunktionen abhängig sein. Für einzelne Funktionen und auch in den aktuell kleineren Testfahrzeugflotten für hochautomatisiertes Fahren werden häufig einfache Ausfallsicherheitskonzepte mit mehrfach redundanter Hardware verwendet. Sobald jedoch Hochautomatisierung für mehrere Funktionen und kostenoptimierte Fahrzeugflotten realisiert werden muss, ist ein allgemeines Konzept für Fail-Operational Verhalten unabdingbar. Welcher Hersteller dies frühzeitig umsetzt und von Insellösungen zu einem generischen Konzept wechselt, erfährt einen technologischen Initialschub und erzielt einen Wettbewerbsvorteil für die Entwicklung zukünftiger Fahrfunktionen. Hierauf ist wohl auch mit Hinblick auf neuartige Geschäftsmodelle durch neue Fahrzeugfunktionen besonderes Augenmerk zu richten. Langfristig bietet eine für den Nutzer unsichtbare Eigenschaft des Bordnetzes sicherlich kein Differenzierungsmerkmal. Daher ist auch in diesem Fall eine einheitliche Lösung und Standardisierung sinnvoll, um Entwicklungskosten für Fail-Operational Verhalten mit der Zeit zu minimieren.

Zukünftige Automobil-Architekturen werden also stärker zentralisiert, hierarchisch und hochintegriert aufgebaut sein. Die Entwicklungen hin zu dienstorientierten Systemen erlauben eine stärkere Flexibilisierung und Adaptierbarkeit. Da auch sicherheitskritische Funktionen von der zunehmenden Automatisierung des Fahrens betroffen sind, ist eine erhöhte Ausfallsicherheit notwendig – von Fail-Silent- zu Fail-Operational-Verhalten. Hierfür können Adaptionen in sichere Fahrzeugkonfigurationen als kostengünstige und flexible Lösung zur Fehlerbehandlung genutzt werden.

Mit Fortschreiten der Automatisierungsgrade und Vernetzung der Fahrzeuge untereinander, mit der Infrastruktur oder der Cloud, werden variablere System-Architekturen entstehen. Das heißt, dass auch Fehlerbehandlungsstrategien und die Betrachtung der Verlässlichkeit über Einzelfahrzeuge hinaus erfolgen müssen. Dafür werden wiederum neue Verfahren zu einer erhöhten Fehlertoleranz und Resilienz der vernetzten Intelligent Transportation Systems benötigt. ■

LITERATURVERZEICHNIS

[1] McKinsey: Automotive revolution – perspective towards 2030, Advanced Industries, 2016.

[2] T. Rosenthal, T. Feismann, P. Schleiß, G. Weiß, and C. Klein: Adaptive Software für sicherheitskritische Funktionen in Batterie-elektrischen Fahrzeugen, AmE 2016, Automotive meets Electronics, VDE/VDI-Gesellschaft Mikroelektronik, Mikro- und Feinwerktechnik -GMM-, 2016.

[3] SAE International: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems (J3016), 2016.

[4] Projekt: Adaptive City Mobility 2. (letzter Zugriff: 14.09.2017)http://www.adaptive-city-mobility.de/

[5] M. Traub, A. Maier, and K. L. Barbehön: Future Automotive Architecture and the Impact of IT Trends, IEEE Software, pp. 27-32, May 2017.

[6] M. Lunt. (2017): AUTOSAR Adaptive Platform Introduction. ASAM General Assembly.

[7] P. Koopman and M. Wagner: Autonomous Vehicle Safety: An Interdisciplinary Challenge. IEEE Intelligent transportation systems magazine, Spring 2017, pp. 90-96.

[8] A. Ruiz, G. Juez, P. Schleiss, and G. Weiss: A safe generic adaptation mechanism for smart cars, IEEE 26th International Symposium on Software Reliability Engineering (ISSRE 2015), 2015.

[9] SafeAdapt: Safe Adaptive Software for Fully Electric Vehicles. http://www.safeadapt.eu (letzter Zugriff: 14.09.2017)

[10] P. Schleiss, C. Drabek, G. Weiss, and B. Bauer: Generic Management of Availability in Fail-Operational Automotive Systems, in: The 36th International Conference on Computer Safety, Reliability and Security, 2017.

[11] G. Weiss, P. Schleiss, C. Drabek, A. Ruiz, and A. Radermacher: Safe Adaptation for Reliable and Energy-Efficient E/E Architectures, in: Comprehensive Energy Management – Safe Adaptation, Predictive Control and Thermal Management. Springer International Publishing, 2018, pp. 1-18.

Gereon Weiß, Dr.
Abteilungsleiter Entwurf & Absicherung Anwendungsarchitekturen, Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik, München
gereon.weiss@esk.fraunhofer.de