André Kohn (Autor)

Virtualisierung und Software-Parallelisierung für Fail-Operational Multicore-Domänensteuergeräte in der Automobilindustrie

https://cuvillier.de/de/shop/publications/7699

1 Elektronikentwicklung und Trends in der Automobilindustrie

Die Verbreitung und Bedeutung von Elektronik als tägliches Hilfsmittel und bei der Verbesserung von bestehenden Technologien steigt in der Gesellschaft kontinuierlich an. Leistungsfähige, informatiklastige IT-Systeme finden vermehrt den Weg auch in die Automobilindustrie, woraus sich neue Herausforderungen für die eher auf Maschinenbau spezialisierten Entwickler ergeben. Zahlreiche unterschiedliche Domänen, die bisher von mechanischen Systemen dominiert wurden, erfahren dabei einen grundlegenden Wandel.

1.1 Anforderungen an zukünftige E/E-Fahrzeugarchitekturen

Fahrzeuge bestanden in der Vergangenheit zum großen Teil aus klassischen, mechanischen Systemen. Ein Wechsel zu mechatronischen Systemen erfolgte durch die Einführung von immer mehr Elektronik und softwarebasierten Systemen. Diese Richtung setzt sich derzeit weiter fort und spiegelt sich in immer komplexeren IT-Systemen, die Einzug in das Fahrzeug erhalten, wider. Heutige E/E-Architekturen verwenden häufig einen modularen Ansatz, bei dem Funktionen durch individuelle Electronic Control Units (ECUs) voneinander isoliert sind. Ein erster Ansatz in Richtung einer optimierten Architektur beinhaltet die Hochintegration von Funktionen auf leistungsfähige Multicore-Controller. Dabei werden bestehende Steuergeräte konsolidiert, wodurch sich eine Einsparung sowohl bei der Steuergeräte-Hardware als auch beim Vernetzungsaufwand ergeben kann. Die aktuelle Entwicklungstendenz verfolgt eine domänenorientierte Zentralisierung auf sogenannte Domain Control Units (DCUs). Diese repräsentieren eine Schnittstelle zu Domänen wie Fahrwerk, Antrieb, Infotainment und Karosserieelektronik, mit dem Ziel einer möglichst einheitlichen Steuergerätearchitektur. Bereits heute sind zahlreiche neue Konzepte in Entwicklung, die Umstrukturierungen der bestehenden Fahrzeugarchitektur beinhalten, um die neue Anforderungen zukünftiger Fahrzeugfunktionen zu erfüllen. Ein Ansatz für weitere Verbesserungen ist eine Fusion bzw. Hochintegration der DCUs zu leistungsfähigen, zentralisierten Fahrzeugcomputern, die in bestimmten Zonen des Fahrzeugs verbaut werden. Die steigende Vernetzung kann zukünftig dazu führen, dass ein Teil der Steuergerätefunktionen in das Backend des Fahrzeugherstellers ausgelagert

wird (Abbildung 1.1). Die grundlegende Herausforderung bei diesen Ansätzen ist die Verbindung der klassischen Fahrzeugeigenschaften mit den umfangreichen Möglichkeiten der IT-Branche.

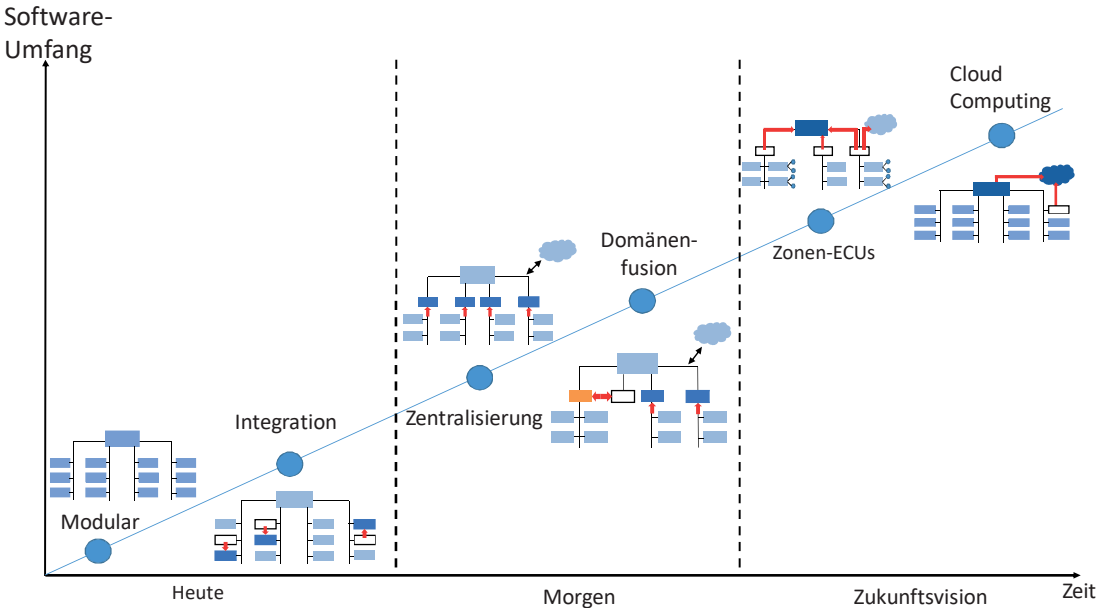

Abbildung 1.1: Evolution des Software-Umfangs in Fahrzeug-E/E-Architekturen

Im Rahmen dieser Arbeit werden unterschiedliche Herausforderungen adressiert, die sich durch eine DCU- und Fahrzeugcomputer-Architektur ergeben. Dazu werden entsprechend potenzielle Lösungsansätze von ausgewählten Themen aufgezeigt.

Grundsätzlich wird die Automobilindustrie mit immer mehr Kundenbedürfnissen und -anforderungen konfrontiert. Die Änderung der E/E-Architektur zu einem Domain Control Unit (DCU)-Ansatz, ist eine erste Maßnahme zur Erfüllung dieser Kundenanforderungen. Als zentraler Kommunikationsknoten kann ein Gateway dienen, das sowohl den Datenaustausch mit dem Backend, als auch zwischen den DCUs ermöglicht. Aufgrund des hohen Datenaufkommens ist eine Anbindung der DCUs an das Gateway über Automotive Ethernet notwendig. Die DCUs übernehmen dabei die Funktion eines zweiten Gateways, das die Kommunikation zwischen dem Ethernet und den entsprechenden Domänenbussen koordiniert. Die Funktionsweise und die Architektur der Steuergeräte innerhalb der Domänen sollen dabei möglichst unverändert übernommen werden. Folglich ist ein Signal-Routing zwischen Ethernet und FlexRay oder CAN(-FD) notwendig. Ein Beispiel für eine domänenbasierte E/E-Architektur ist in Abbildung 1.2 dargestellt.

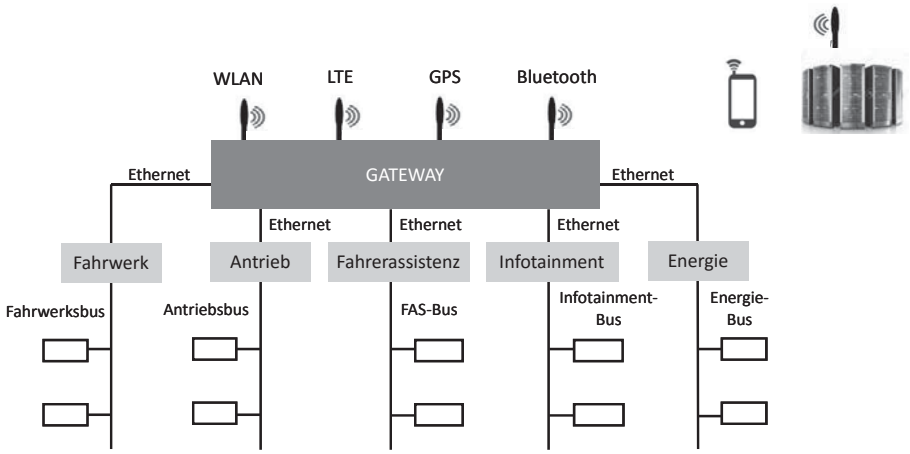

Abbildung 1.2: Beispiel für eine domänenbasierte E/E-Architektur

Die mit dieser E/E-Architektur zu erfüllenden Anforderungen werden in den folgenden Abschnitten beschrieben.

Online-Aktualisierung von Steuergerätesoftware

Eine wesentliche Neuerung der nächsten Fahrzeuggeneration ist die Möglichkeit, zusätzliche Funktionen nachträglich ins Fahrzeug einzubringen. Dies erfordert eine Infrastruktur mit einem ausgereiften OEM-Backendkonzept und der Kommunikationsanbindung über Mobilfunkstrecken. Zudem müssen die heutigen Steuergerätearchitekturen sowie die Vernetzungsarchitektur des Fahrzeugs überarbeitet werden, so dass der Kunde Funktionen bei Bedarf nachladen kann. Diese können zum einen bei der Fahrzeugauslieferung an den Kunden in Entwicklung sein oder noch nicht existieren. Zum anderen ist es vorstellbar, dass Funktionen im Fahrzeug bei der Fahrzeugauslieferung an den Kunden bereits vorinstalliert sind und nachträglich entgeltlich für einen definierten Zeitraum aktiviert werden. Denkbar sind Assistenzfunktionen oder eine gesteigerte Motorleistung für ein komfortableres oder sportlicheres Fahrerlebnis. Ein weiterer Anwendungsfall für das nachträgliche Einbringen von Software ist eine Softwareaktualisierung, wodurch potenzielle Security-Lücken geschlossen werden, um das Fahrzeug gegen unerlaubte Zugriffe und Manipulation zu schützen. Insbesondere die Anbindung von externen Geräten zur Kommunikation mit dem Fahrzeug oder zur direkten Fahrzeugsteuerung eröffnet Hackern viele neue Möglichkeiten, Zugriff auf das Fahrzeug zu erhalten.

Personalisierung und Profilierung

Bereits heute ist es durch vorgegebene Profile möglich das Fahrverhalten des Fahrzeugs von komfortabel, energieeffizient bis zu sportlich einzustellen. Durch die neue Fahrzeugarchitektur kann der Fahrer einerseits ein eigenes Profil im Fahrzeug individuell erstellen. Dabei gilt es genau abzuwägen, welche Fahrzeugparameter einstellbar sein sollen und mit welchen Möglichkeiten der Fahrer überfordert sein könnte. Andererseits können mit Hilfe der Daten, die während der Fahrt gesammelt worden sind, personalisierte Fahrzeugeinstellungen für ein verbessertes Fahrerlebnis vorgeschlagen werden. Die Personalisierung beinhaltet außerdem zusätzliche Funktionsempfehlungen, die für den Fahrer interessant sein könnten.

Datensammlung für vernetzte Fahrzeugfunktionen

Die Datenerfassung und -sammlung über den Fahrzeugzustand sowie des Fahrers ist ein weiteres Ziel in zukünftigen Fahrzeugen. Ein Großteil kommender Fahrzeugfunktionen sind abhängig von Daten die entweder durch andere Fahrzeuge, durch die Verkehrsinfrastruktur oder vom Backend bzw. der Cloud zur Verfügung gestellt werden. Häufig sind diese Funktionen nur möglich, wenn die Verkehrsinfrastruktur ebenfalls durch intelligente Elektronik erweitert wird (Parkhauspilot, Ampelassistent). Auch Assistenzfunktionen, die ein automatisiertes Fahren ermöglichen, erfordern zahlreiche Daten aus der Fahrzeugsensorik, die mit Backenddaten fusioniert werden. Weitere Konzepte beschreiben die Sammlung von Umgebungsdaten wie Straßenbeschaffenheit oder Luftqualität durch die Fahrzeugsensorik. Mit Hilfe dieser von dem Backend gelieferten Daten können nachfolgende Fahrzeuge beispielsweise ihre Dämpferregelung oder Innenraumklimatisierung prädiktiv anpassen.

Security-Mechanismen

Nahezu jede der zukünftigen Fahrzeugfunktionen benötigt Security-Mechnismen, die bis heute nur durch wenige Funktionen wie beispielsweise Wegfahrsperre oder Tuningschutz realisiert werden. Dazu zählt unter anderem die Kommunikation zwischen mobilen Geräten, die entweder mit einer direkten Verbindung oder über ein Backend und Mobilfunknetz erfolgen kann. Ein Steuergerät dient hier als Schnittstelle zwischen den Kommunikationsbussen des Fahrzeugs und dem Backend, so dass die Software- und Hardwarearchitektur entsprechend angepasst werden muss. Ein weiterer Anwendungsfall für Security ist die Sicherheit von Flashdaten für die Steuergeräte. Dabei existiert ein deutlicher Unterschied bei der Vorgehensweise im Infotainment und den klassischen ECUs. Während ein leistungsfähiges Infotainmentsteuergerät häufig über externe Medien geflasht wird,

ist dies bei ECUs mit harten Echtzeitanforderungen derzeit nur über die Diagnoseschnittstelle möglich. Bei Mikrocontrollern mit sicherheitsrelevanten Funktionen wird die Steuergerätesoftware aufgrund des geringen Speichers zunächst geflasht und danach verifiziert. Da durch das flexible Funktionsnachladen auch ein Rückflashen möglich sein muss, sind hier neue Konzepte notwendig. Weitere Security-Mechanismen für den Manipulationsschutz sind die Absicherung der Fahrzeugdiagnose sowie die Onboard-Kommunikation. Zur sicheren Schlüsselablage und Zertifikatsverwaltung wird außerdem ein Key Management System (KMS) benötigt.

Generell bestehen die Schutzklassen im Fahrzeug aus den Punkten *Safety*, *Geld & Geschäft*, *Datenschutz & Gesetze* und *Qualität* (Abbildung 1.3).

Abbildung 1.3: Security-Schutzklassen der Automobilindustrie

Safety zielt auf den Schutz der Fahrzeuginsassen und den anderen Verkehrsteilnehmern ab. Das Ziel ist die Gewährleistung der allgemeinen Betriebssicherheit und Zuverlässigkeit des Fahrzeugs und seiner Funktion. Bei einer Security-Lücke entsteht eine **Gefahr für Leib und Leben**.

Datenschutz & Gesetze konzentriert sich auf den Datenschutz der Kunden des Automobilherstellers. Ein unerlaubter Zugriff führt zu einer Verletzung der **Privatsphäre des Kunden sowie einem potentiellen Missbrauch der Kunden- und Herstellerdaten**.

Die Freischaltung von kostenpflichtigen Funktionen, beispielsweise bei Software as Product (SWaP), ist Bestandteil der Schutzkategorie *Geld & Geschäft*. Ein Auslesen von Fahrzeugdaten kann zu einem Verlust der Intellectual Property (IP) des Herstellers sowie zu einer generellen Gefährdung des Geschäftsmodells und folglich einem erheblichen **finanziellen Schaden des Herstellers** führen.

Bei einem Angriff auf die Produktqualität fallen einzelne Komponenten oder Fahrzeugfunktionen durch Manipulation aus oder liefern falsche Daten. Dies kann dazu führen, dass der Kunde die Qualität des gesamten Fahrzeugs anzweifelt. Ein Beispiel sind korrupte Anzeigen im Kombiinstrument oder ein Versagen des Fahrzeugs. Dadurch steigt die Wahrscheinlichkeit, dass der Kunde zukünftig auf