Neue Konzepte für zukünftige E/E-Architekturen

Zukünftige Fahrzeuge stehen aufgrund der sich rasant wandelnden Mobilität völlig neuen Herausforderungen gegenüber. Insbesondere die Anforderungen an die kommenden E/E-Architekturen verändern sich ständig. Im EU-geförderten Projekt SafeAdapt haben neun Partner aus sechs Ländern untersucht, inwiefern Adaptivität für flexible und zuverlässige E/E-Architekturen genutzt werden kann.

© Fraunhofer ESK/Bernd Müller

Die Mobilität von morgen wird geprägt sein von einem deutlich höheren Anteil der Elektromobilität, zunehmender Automatisierung sowie dem Wandel hin zur Mobilität als Dienst. Dabei spielt vor allem die Software als hauptsächlicher Wegbereiter von Innovationen eine zentrale Rolle. So kann durch Software eine erhöhte Verlässlichkeit und Flexibilität des Fahrzeugbordnetzes erzielt werden. Um dies zu belegen und zu demonstrieren, wurden im SafeAdapt-Projekt neue Konzepte für eine zukünftige E/E-Architektur erforscht. Im Mittelpunkt standen verschiedene Anwendungsfälle, etwa Ausfallsicherheit im Fehlerfall, erhöhte Energieeffizienz oder Plug'n'Play-Szenarien. Darauf aufbauend erarbeiteten die Projektpartner neue Lösungen mit einer adaptiven Software-Architektur.

Neue Konzepte für zukünftige E/E-Architekturen

Die in SafeAdapt entstandenen neuen Architekturkonzepte beruhen auf speziellen Prinzipien, die eine adaptivere Bordnetzarchitektur ermöglichen. Um kosteneffizient die Verlässlichkeit zu erhöhen, wird eine Software-basierte Redundanz verwendet. Diese setzt jedoch eine zugrundeliegende Redundanz von Teilen der Hardware-Architektur voraus. Um beispielsweise den Ausfall eines Steuergeräts durch ein anderes kompensieren zu können, müssen auch im Fehlerfall benötigte Sensoren und Aktuatoren von einzelnen Steuergeräten unabhängig verbaut sein. Eine solche Absetzung der Sensorik und Aktuatorik wird auch heute schon durch die zentrale Aggregation von Umfeldinformationen forciert. Um auch die Kommunikation zwischen sicherheitskritischen Komponenten bei Störungen wie einem Kabelbruch zu gewährleisten, sind redundante Kommunikationspfade zwischen allen ausfallsicheren Komponenten unerlässlich. Damit eine Stromquelle als Single-Point-of-Failure ausgeschlossen werden kann, muss diese auch zusätzlich abgesichert sein, z. B. durch eine ebenfalls redundante Auslegung.

Aufbauend auf dieser Architektur, wurde im Projekt ein übergreifender Sicherheitsmechanismus entwickelt, der allgemein von allen sicherheitsrelevanten Funktionen genutzt werden kann. Das ermöglicht der sogenannte Safe Adaptation Platform Core, kurz SAPC (Bild 1). Dieser kann flexibel Systemkonfigurationen aktivieren, um zum Beispiel im Fehlerfall in eine Konfiguration zu wechseln, die trotzdem alle sicherheitskritischen Funktionen des Fahrzeugs sicherstellt. Das vorgestellte Konzept lässt sich für diverse individuelle Architekturen anpassen und optimieren. Der SAPC wurde auch als AUTOSAR-Komponente entwickelt und kann so auf

verschiedenen Plattformen verwendet werden. Dies umfasst AUTOSAR OSEK, aber auch mächtigere Echtzeitbetriebssysteme, die im Projekt Verwendung fanden.

Prototypenstudien und Demonstratoren

Um zu demonstrieren, dass die neuen Konzepte umsetzbar sind und um ihre Eignung zu überprüfen, haben die Projektpartner verschiedene Analysen durchgeführt und Prototypen aufgebaut. So wird auch die Systementwicklung durch Software-Werkzeuge für Entwurf und Analyse gezielt unterstützt. Dabei lässt sich die Adaptivität in der Software-Architektur mit der Modellierungssprache EAST-ADL und im Projekt erarbeiteten Erweiterungen beschreiben.

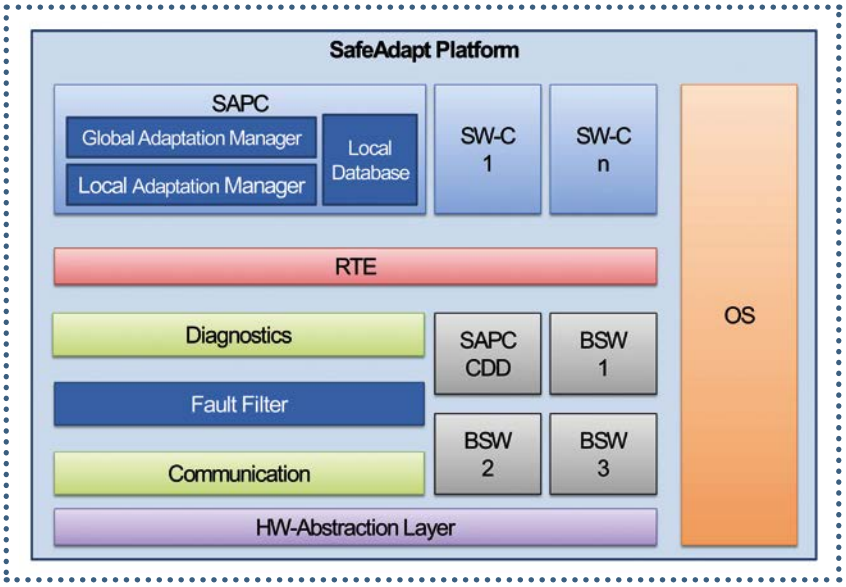

Bild 1: Schematischer Aufbau der SafeAdapt-Steuergeräte-Architektur.
(© Fraunhofer ESK)

Diese Architekturmodelle können wiederum dafür genutzt werden, die adaptiven Eigenschaften zu validieren. Hierfür wurden beispielsweise Methoden für Simulationen mit verschiedenen Frameworks umgesetzt, um mit einer sogenannten Fault-Injection die Auswirkungen von Fehlern sowie die korrekte Reaktion der Adaption nachzuvollziehen. Das heißt: Es wurde unter anderem untersucht, ob das System für alle zu berücksichtigenden Fehler in die jeweils richtige Fehlerkonfiguration wechselt.

Für die Bestimmung aller notwendigen Konfigurationen kommt ein im Projekt erstelltes, automatisiertes Planungstool zum Einsatz. Unter anderem ist es damit auch möglich, flexiblere Architekturen integriert mit aktuellen AUTOSAR-Werkzeugketten zu entwickeln: Basierend auf den Anforderungen aus dem Entwurf und der Safety-Analyse werden gültige AUTOSAR-Konfigurationen automatisch generiert, die alle definierten Randbedingungen berücksichtigen. Die für die Fehlerbehandlung notwendigen Informationen werden zusätzlich erzeugt. Ein Modellauto veranschaulicht dies: Es liefert den Nachweis durch eine ausfallsichere elektronische Lenkung mit aktuellen AUTOSAR-Classic-Plattformen, basierend auf den erforschten Konzepten.

Darüber hinaus können in Form eines Driver-in-the-Loop-Simulators kritische Szenarien in einer virtuellen Umgebung evaluiert werden. So liefern Fahrerstudien zum Beispiel Erkenntnisse darüber, wie viel Zeit zur Kompensation eines Fehlers, etwa der Ausfall der Lenkfunktion, vergehen kann, bis der Fahrer es bemerkt oder die Kontrolle über die Fahrzeugführung verliert. Zudem wurde mittels des Simulators ein Szenario zur Nutzung der Adaption für eine erhöhte Energieeffizienz untersucht. In diesem Fall lassen sich aktuell nicht verwendete und nicht notwendige Software- und Hard- »

ware-Funktionen abschalten. Dieses Szenario zeigt, dass bei einem geringen Batteriestand das System in eine energieoptimierte Konfiguration wechselt, um ein Fahrziel noch zu erreichen.

Um die Konzepte in einer realen Systemumgebung zu demonstrieren, wurden diese in ein E-Fahrzeug integriert. Zu diesem Zweck haben die Projektpartner das Auto mit der SafeAdapt-E/E-Architektur und mit über Echtzeit-Ethernet verbundenen Steuergeräten umgerüstet. Hierdurch können verschiedene Szenarien im realen Fahrzeug untersucht werden. Ein Beispiel dafür ist die Ausfallsicherheit einer sicherheitskritischen Funktion wie Steer-by-Wire. Darüber hinaus stellt die Adaptivität des Systemverbunds sicher, dass verschiedene, in der Safety-Analyse identifizierte Einzelfehler kompensiert werden. So ist beispielsweise die Lenkfunktion beim Ausfall des Steuergeräts, auf dem diese Funktion primär ausgeführt wird, oder bei Störung einer relevanten Kommunikationsverbindung weiterhin sichergestellt.

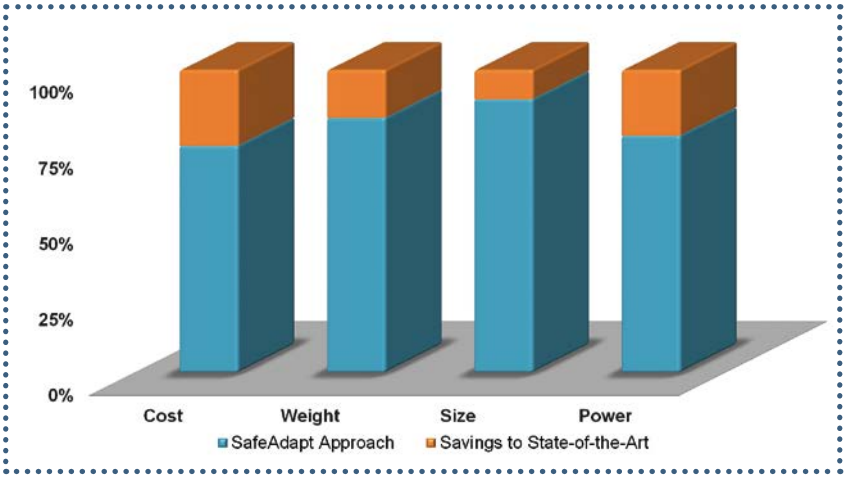

Bild 2: Vergleich der Einsparungen eines Beispiel-Fahrzeugsystems mit der SafeAdapt-Architektur. (© Fraunhofer ESK)

Ergebnisse

Die erarbeiteten Konzepte ermöglichen eine flexiblere und verlässlichere E/E-Architektur, wie sie für Anforderungen an zukünftige Fahrzeuge benötigt wird. Durch die Untersuchungen mithilfe der verschiedenen Prototypen konnten die Ansätze analysiert und belegt werden. So wurde beispielsweise im Rahmen der Fahrerstudien in den Driver-in-the-Loop-Simulationen herausgefunden, dass ein Ausfall der Steer-by-Wire-Lenkung für den Fahrer funktional nicht bemerkbar ist. Erst ab einer höheren Ausfalldauer von größer 150 ms wurde der Fehler qualitativ wahrgenommen und ab 250 ms als sicherheitskritisch bewertet. Die vorgestellte Lösung ist durch Vorberechnungen in der Lage, solche Fehler in deutlich weniger Zeit zu behandeln.

Zudem ermöglicht der vorgestellte Ansatz einen allgemeinen Fehlerbehandlungs-Mechanismus, der unabhängig von der einzelnen Funktionsentwicklung verwendet werden kann. Das heißt: Nicht jede sicherheitskritische Funktion muss individuell um Ausfallsicherheit erweitert werden. Vielmehr kann dafür auch der allgemeine Sicherheitsmechanismus gemäß ISO 26262 verwendet werden. Letzteres war spezieller Gegenstand von Untersuchungen. Dabei wurde insbesondere auch analysiert, inwiefern sich der aktuelle Sicherheitsstandard für noch stärker adaptive Fahrzeugsysteme eignet.

Eine Berechnung der Ressourcen für eine Systemauslegung nach den oben genannten Ansätzen und bisherigen Standardarchitekturen anhand einer Beispielarchitektur zeigt das große Potenzial (Bild 2). Allerdings kann dies natürlich nur im Einzelfall für jede E/E-Architektur individuell verlässlich bestimmt werden.

Ausblick

Flexible und ausfallsichere E/E-Architekturen sind für künftige Mobilität unerlässlich. Das mit SafeAdapt vorgestellte Lösungskonzept zeigt, dass sich dies in realen Systemen effizient umsetzen lässt. Insbesondere die mit großen Schritten voranschreitende Automatisierung macht solche Konzepte dringend erforderlich. Sobald der Fahrer, wie ab dem Status der Hochautomatisierung und darüber hinaus, das Fahrzeug nicht mehr ständig überwachen muss, sind kosteneffiziente Architekturlösungen für erhöhte Ausfallsicherheit unerlässlich. Aus diesem Grund zeichnet sich die Übernahme solcher Ansätze in die nächsten Generationen automatisierter Fahrzeuge bereits heute ab. ■ (oe)

» **www.esk.fraunhofer.de**

Dr. Gereon Weiß ist stellvertretender Geschäftsfeldleiter Automotive bei Fraunhofer ESK und Koordinator des SafeAdapt Projekts.

Dipl.-Ing. Thorsten Rosenthal ist Senior Systems Engineer Advanced Engineering im Bereich Body & Security bei Delphi.