Fraunhofer
ESK

FRAUNHOFER-INSTITUT FÜR EINGEBETTETE SYSTEME UND KOMMUNIKATIONSTECHNIK ESK

Adaptive Software-Architektur für Fahrzeuge

Mit dem Aufkommen elektrischer Antriebe steht die Automobilbranche vor neuen Herausforderungen. Der Einsatz rein elektrischer Antriebe legt den Wechsel zur vollständig elektrischen Steuerung vieler Funktionen nahe. Dies erfordert eine grundlegende Änderung der Systemarchitektur des Fahrzeugs. Hochintegrierte Subsysteme, wie Radnabenmotoren und X-by-Wire Systeme, sind im höchsten Maße sicherheitsrelevant. Folglich steigt die Komplexität der E/E-Architektur von Fahrzeugen deutlich.

Im von der Europäischen Union geförderten Projekt SafeAdapt (Safe Adaptive Software for Fully Electric Vehicles) überarbeiten die neun Partner aus sechs Ländern die E/E-Architektur, welche die Komplexität auf das notwendige Maß reduziert sowie Kosten- und Energieeffizienz erhöht. Dabei soll durch eine generische und systemweit einheitliche Fehlerbehandlung basierend auf der Adaption des Systems zur Laufzeit die Systemkomplexität reduziert werden. Dies erhöht die Zuverlässigkeit gegenüber Fehlern und optimiert den Ressourcenbedarf. Dabei wird in SafeAdapt ein ganzheitlicher Ansatz für den Einsatz adaptiver Systeme in sicherheitskritischen Umgebungen erarbeitet.

Safe Adaptation Platform Core sorgt für effiziente Redundanz

Vollständig elektrisch betriebene Automobile haben spezifische Anforderungen – besonders bezüglich Sicherheit und Zuverlässigkeit. So kann z.B. bei Verwendung eines elektrischen Radnabenmotors keine Kupplung den Motor vom Antriebstrang trennen. Die Software zur Kontrolle des Antriebs muss somit das spezifizierte Verhalten auch im Fehlerfall sicherstellen, um das Auto im Notfall sicher zu stoppen.

Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik ESK

Hansastr. 32
80686 München

Ansprechpartner

Dr. Gereon Weiß
Telefon: +49 89 547088-348
gereon.weiss@esk.fraunhofer.de

Dr.-Ing. Dirk Eilers
Telefon: +49 89 547088-329
dirk.eilers@esk.fraunhofer.de

www.esk.fraunhofer.de

Der Safe Adaptation Platform Core kombiniert verschiedene Hardware-Plattformen mit einer adaptiven Netzwerkinfrastruktur, um die Anforderungen hoch sicherheitskritischer Systeme an Redundanz kosteneffizient zu erfüllen. Dieser Ansatz ermöglicht eine generische Fehlerbehandlung basierend auf der Fähigkeit des Systems sich zu rekonfigurieren. Dadurch kann ein sogenanntes fail-operational Verhalten der E/E-Architektur effizient umgesetzt werden. Zusätzlich ermöglicht eine generische Behandlung von Fehlern mittels Adaption eine signifikante Verbesserung der Wiederverwendbarkeit von Software in Fahrzeugen.

SafeAdapt liefert Entwurf und Systemarchitektur

Um die sichere Adaption der Software zur Laufzeit zu gewährleisten, muss das spezifizierte Verhalten des Systems in unterschiedlichen Modi und Konfigurationen zur Laufzeit bekannt und validiert sein. Die Spezifikation der Adaptation im Entwurf umfasst die Definition verschiedener Konfigurationen, der notwendigen Anpassungen sowie der Anforderungen, z.B. die maximal zulässige Verzögerung zum Wechsel zwischen den definierten Konfigurationen. In SafeAdapt wird die Adaption während des Entwicklungsprozesses durch bereits existierende Modellierungssprachen beschrieben, wie UML, EAST-ADL oder AUTOSAR. Hierdurch ermöglicht der Ansatz eine frühzeitige Verifikation und Validierung der nicht-funktionalen Systemeigenschaften wie der Adaptivität. Auf dem Systemmodell aufbauend können automatisiert gültige Konfigurationen generiert werden, die alle Fehlerszenarien berücksichtigen. Dies geschieht konform zum AUTOSAR Standard, was wiederum die Anwendbarkeit für verschiedene Electronic Control Units (ECUs) und Nutzung von Standard Werkzeugketten erleichtert.

Weiterverwendung von Software Komponenten durch Zertifizierung

Eine weitere Herausforderung ist die Notwendigkeit einen Zertifizierungsprozess entsprechend dem funktionalen Sicherheitsstandard ISO26262 für jedes Fahrzeugmodell neu durchzuführen. SafeAdapt adressiert dies, durch die Analyse und Verwendung entsprechender Konzepte der ISO26262, wie dass Safety Element out of Context (SEooC) Konzept. Das letztere erlaubt es, Softwarekomponenten in verschiedenen Fahrzeugmodellen wiederzuverwenden, ohne diese in jedem neuen System erneut zu zertifizieren. Beispielsweise wird der im Projekt entwickelte Safe Adaptation Platform Core als SEooC definiert, wodurch er nur einmal verifiziert werden muss und für verschiedene Plattformen genutzt werden kann.

Proof-of-Concept durch ein Prototypenfahrzeug

Der in SafeAdapt entwickelte Ansatz soll:

- Komplexität und Hardware-Kosten reduzieren,
- Fehler in sicherheitskritischen Systemen durch Adaption bzw. Rekonfiguration behandeln und
- Entwicklungs-, Test- und Zertifizierungskosten reduzieren.

Um die Projektergebnisse unter realen Bedingungen zu evaluieren, werden die erarbeiteten Konzepte sowie die im Projekt entstehenden Komponenten in ein existierendes elektrisches Prototypenfahrzeug integriert. Darüber hinaus wird der SafeAdapt Ansatz in einer Fahrzeugsimulationsumgebung validiert und evaluiert.

Support & Service

Das Fraunhofer ESK bietet seine langjährige Erfahrung im Bereich zukünftiger E/E-Architekturen an, um es Kunden zu ermöglichen, solches erweitertes fail-operational Verhalten in ihre Produkte zu integrieren. Dies kann von ersten Studien über den Entwurf, Software-Werkzeugimplementierungen bis zu vollständigen Prototypen reichen. Sprechen Sie uns an, um mögliche Kooperationen zu diskutieren, die Ihren Anforderungen und Wünschen entsprechen.

Das Projekt wird von der Europäischen Kommission im Rahmen des European Union's Seventh Framework Programm (FP7) gefördert - Grant agreement No 608945

PDB_SafeAdapt_dt
Feb 2016