SW-basierte Integration von neuen Fahrzeugfunktionen in zentralisierten Controllern

Klaus Becker[1], Christian Buckl[1], Alexander Camek[1], Rainer Falk[2], Ludger Fiege[2], Jürgen Geßner[2], Stephan Sommer[1]

1) fortiss gemeinnützige GmbH, Guerickestraße 25, 80805 München

2) Siemens AG, Corporate Research and Technologies, Otto-Hahn-Ring 6, 81730 München

Abstract

In aktuellen Fahrzeugen wird ein wesentlicher Teil der Fahrzeugfunktionen durch Software realisiert. Hochintegrierte Elektromotoren und die Integration aktiv eingreifender Assistenzsysteme werden diesen Trend noch verstärken. Das zugrunde liegende Bordnetz, auf dem die Software ausgeführt wird, ist historisch gewachsen und wird durch den zunehmenden Funktionsumfang immer komplexer. In diesem Artikel stellen wir einen Ansatz vor, Bordnetz und Software im Fahrzeug über eine datenzentrische Middleware zur Laufzeit zu koppeln. Der Ansatz basiert auf einer Zentralrechnerarchitektur, die eine fail-operational Ausführung von Funktionen erlaubt. Die datenzentrische Middleware koordiniert die Kommunikation zwischen Funktionen, Sensorik und Aktorik zur Laufzeit. Eine Vermittlung der Datenzugriffe ähnlich einer „virtuellen Datenbank“ unterstützt die Entkopplung von Funktion und Netzwerk unter Berücksichtigung von Echtzeit-, Redundanz- und Erweiterbarkeitsanforderungen. Wir stellen am Beispiel Plug-and-Play (PnP) eine neue Sekundärfunktion vor, die durch diesen Ansatz ermöglicht wird. Security-Aspekte der vorgestellten Architektur werden ebenfalls betrachtet.

1 Einführung und Motivation

Heutige Automobile sind ein komplexes Zusammenspiel von verteilen, gekoppelten Einzelsystem. Derzeitige Premiumfahrzeuge enthalten eine hohe Anzahl von bis zu ca. 100 Steuergeräten (Electronic Control Units, ECUs), die mit verschiedenen Bussystemen miteinander verbunden sind. Selbst wenn Funktionen in *Domänenkontrollern* konsolidiert werden, so ist der entstehende Verkabelungsaufwand jedoch enorm und wächst weiter an mit jedem für eine neue Fahrzeugfunktion hinzukommenden Steuergerät, das in die vorhandene Infrastruktur integriert werden muss. Zukünftiger Bedarf, Assistenz- und Komfortsysteme stärker mit dem Antriebsstrang zu kombinieren, wird diese Entwicklung weiter forcieren.

Ein weiterer Treiber der Domänen übergreifenden Integration sind hochintegrierte Radnaben- oder radnahe Elektromotoren. Ihre geringe Baugröße und der hohe Funktionsumfang können zu einem neuen Zuschnitt der Funktionsverteilung in Mehrmotor-Fahrzeugen führen. Die Integration von Lenkung, Vortrieb, Verzögerung wie auch von ABS und ASR in ein einziges, autark arbeitendes Modul, lässt Differenzial, Torque-Vectoring sowie die Beschleunigung selber zu einer verteilten Steuerung werden in der die Funktionen der Module zentral koordiniert werden müssen.

Die sichere (safe und secure) Integration der Rechner sowie der notwendigen Sensoren und Aktoren ist ein treibender Faktor für Entwicklungskosten und -zeit. Der steigenden Komplexität wird typischerweise mit einer Konsolidierung begegnet, wie sie mit dem Wechsel von diskreten Datenleitungen hin zu Bussystemen in der Automobiltechnik erfolgte (vgl. Abbildung 1 sowie [7]). Als Lösungsmöglichkeiten für vergleichbare Herausforderungen sind in Avionik, Industrieautomatisierung und Robotik zentralisierte Architekturen entworfen worden, die auch bereits in automobilen Forschungsprojekten angewendet wurden (vgl. [12] und [13]). Die Entwicklung neuer Funktionen konzentriert sich dann auf die SW-Integration und die Kopplung der Sensorik/Aktorik an ein Backbone-Netzwerk (vgl. [6], [10]). Den Zugriff auf die notwendigen Daten übernimmt eine Kommunika-

tionsschicht (Middleware), die Sicherheits- und Qualitätsziele garantieren muss, die heute durch separierte Bussysteme erbracht werden.

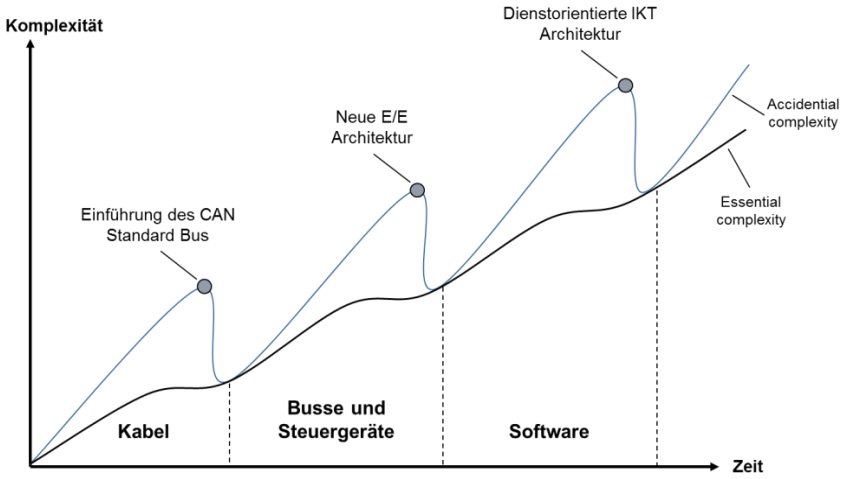

Abbildung 1: Wachsende Komplexität durch inkrementelle Weiterentwicklung [7]

In diesem Artikel möchten wir einen Ansatz für eine datenzentrische Middleware aufzeigen, die es erlaubt, Sensoren und Aktoren von den verarbeitenden Funktionen zu entkoppeln. Basierend auf vorverarbeitender, intelligenter Peripherie, werden Daten in aufbereiteter Form in einer Datenbank abgelegt und Steuergeräte übergreifend zur Verfügung gestellt. Als wesentlicher Treiber wird die Integration neuer Softwarefunktionen auch nach Auslieferung des Fahrzeugs betrachtet.

Eine Rekonfiguration der IKT-Ressourcen (CPU, Netz, Datenzugriff) erfolgt automatische im System. Wichtige Randbedingungen sind die Einhaltung von Safety-und Security-Anforderungen. Das System soll sowohl um neue Software (Fahrzeugfunktionen), als auch um neue Hardware (Sensoren, Aktoren und Steuergeräte) erweitert werden können.

Die hier vorgestellten Konzepte sind kein Ersatz für AUTOSAR, sondern konzentrieren sich auf die Kombination von Erweiterbarkeit (zur Laufzeit) sowie Safety Mechanismen in einer geschichteten Architektur, die die Entwicklung von Applikations- und Sicherungsfunktionalität trennt. Unsere Konzepte sind zunächst orthogonal zu AUTOSAR und könnten daher zukünftig als eine mögliche Erweiterung angesehen werden. Die Validierung der Konzepte erfolgt im Rahmen des RACE Projektes mit Hilfe von Fahrzeug-Prototypen [3].

Der Aufsatz ist wie folgt strukturiert: Kapitel 2 stellt zunächst die zugrunde liegende zentralisierte Systemarchitektur vor. In Kapitel 3 wird der datenzentrische Ansatz vorgestellt. Neue Funktionen, die durch die Architektur ermöglicht werden, werden in Kapitel 4 beschrieben und Kapitel 5 schließt mit einer Zusammenfassung.

2 Zentralisierte Systemarchitektur

Ein Kern der Systemarchitektur, die sie hier an Avionik und Industrieautomatisierung orientiert, ist eine deutlich horizontale Schichtung der Architektur. Die heute vorherrschende Bündelung von Funktion, ECU, Sensorik in Teilsystemen wird ersetzt von einer Aufteilung in Feldebene zur Anbindung von Sensorik/Aktorik, lokalen Regelung von Stellgrößen (Motoren) und koordinierenden bzw. planenden Aufgaben in der Steuerungs- bzw. Leitebene.

Die betrachtete Systemarchitektur umfasst zentrale Rechner für koordinierende Aufgaben, ein Ethernet-basiertes Backbone und intelligente Sensoren/Aktoren, die direkt oder via Sektor-Gateways (z.B. für den Frontbereich) angeschlossen sind. Grundsätzliches Merkmal der zentralen

Rechner ist in allen Fällen, dass sie keine funktionsspezifischen Ein/Ausgaben (ADC, spezielle Busse, etc.) besitzen, sondern lediglich an das Backbone-Netzwerk angeschlossen sind.

Die Zentralrechner übernehmen das vorausschauende Planen und setzen zusätzlich modulübergreifende, überlagerte Regelungen und koordinierende Funktionen um [2]. Sie bilden beispielsweise den Fahrvektor aus den Vorgaben des Fahrers und der Assistenzfunktionen und setzen diese in Leistungsanforderungen (Zielwerte) an die Motoren (Aktoren) um. Die Radmodule bestehen aus E-Motoren, Inverter und lokaler Regelung, die schnelle, geschlossene Regelungsaufgaben übernimmt und die Zielwerte von den Zentralrechnern erhält. In Zukunft können die Radmodule auch Grundfunktionen der Blockier- und Schlupfregelung übernehmen, jedoch enthalten diese Module prinzipiell keine koordinierenden Aufgaben zwischen anderen Aktoren bzw. Aufgaben, die nichts mit ihrer lokalen Kontrolle physikalischer Größen zu tun haben.

Die hohe Integration eines Elektroradmoduls lässt sich hervorragend mit einer X-by-Wire Architektur kombinieren. Eine beispielhafte Darstellung für ein X-by-Wire-Fahrzeug ist in Abbildung 2 dargestellt.

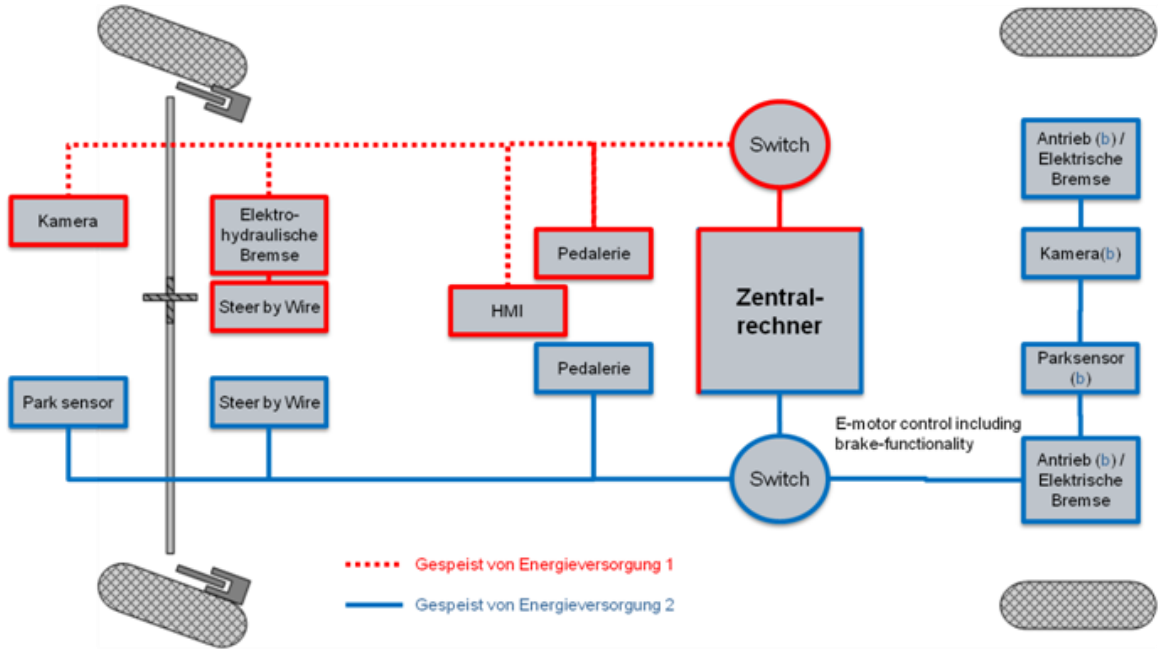

Abbildung 2: Übersicht Systemarchitektur mit logisch zentralem Rechner

Da es für ein fahrendes Automobil keinen sicheren Zustand gibt, müssen sicherheitskritische Funktionen, wie z.B. Lenkung und Bremse, ASIL-D Anforderungen erfüllen. Dies betrifft sowohl die Kommunikation als auch die Zentralrechner und die Energieversorgung. Gemäß der ISO 26262 Anforderungen muss die Wahrscheinlichkeit eines fehlerfreien Betriebs bei Einzelfehlern bei >99% bzw. für Mehrfachfehler bei > 90% liegen und das bei einer Fehlerrate von weniger als 10^{-8} /h.

Es gibt mehrere Architekturkonzepte die ASIL-D Anforderungen mit Fail-Operational Verhalten erreichen: Wir wählen einen Duo-Duplex-Aufbau. Jeweils ein Paar zentraler Rechner ist in einem Duplex Control Computer (DCC) verbunden, um die Ein/Ausgangsdaten gegenseitig zu überwachen und Inkonsistenzen festzustellen. Ein zweites Paar (zweiter DCC) läuft als hot-standby, um im Fehlerfall die Funktionalität aufrecht zu erhalten. Der Duo-Duplex-Ansatz lässt sich im Vergleich zu Triplex-Systemen leichter skalieren und die Aktoren benötigen kein systemisches Wissen und keine an den Grad der Redundanz gebundenen „Voter“ zur Fehlererkennung.

Das Netzwerk muss ebenfalls redundant aufgebaut werden. Hier kommt eine Ringtopologie zum Einsatz, wie sie in der Industrietechnik (Profinet) sowie Schutz und- Leittechnik (IEC 61850) bevorzugt wird. Für Details sei auf [1] verwiesen.

Aus den Verantwortlichkeiten der Sensoren/Aktoren und der Zentralrechner (DCC) ergibt sich, dass Zustands- und Sensordaten über das Netzwerk den Applikationen in den DCCs zur Verfügung gestellt werden müssen. Umgekehrt müssen die errechneten Zielwerte den Aktoren übermittelt werden. Als Zykluszeit für den regelmäßigen Austausch dieser Daten ergibt sich ein Richtwert aus den Erkenntnissen der Projekte Sparc und HAVEit. Dort waren zentralisierte, koordinierende Funktionen mit einer Zykluszeit im Bereich von 10-20ms für betrachtete Fahrsituationen eines PKW ausreichend. Die datenzentrische Middleware muss also die Elemente der Systemarchitektur (Sensoren, Aktoren, DCCs) verbinden und adressiert dabei folgende Ziele:

- Echtzeitfähigkeit (Zykluszeit 10ms)
- Erweiterbarkeit
- Mixed-criticality (Kombination QM bis ASIL-D, fail-operational)

2.1 Relation zu AUTOSAR

Die hier vorgestellten Ansätze sowohl von der Systemarchitektur und der datenzentrischen Middleware ermöglichen die Analyse und Entwicklung neuer Ansätze der Erweiterbarkeit und Safety im Automotive Umfeld. Die skizzierten Ansätze können als eine mögliche Erweiterung des AUTOSAR Standards betrachtet werden.

Die vorgestellte Architektur schreibt systemische Redundanzen vor, die so im AUTOSAR Standard nicht gefordert werden. Dies erlaubt zum einen Sicherungsmechanismen zu entwerfen, die HW-Fehler unabhängig von den Applikationen erkennen und behandeln. Dies beinhaltet auch den mixed-criticality Betrieb, in dem Anwendungen unterschiedlicher Safety-Levels auf einer DCC laufen und kommunizieren können. Desweiteren wird die datenzentrische Middleware oberhalb der AUTOSAR RTE-Funktionalität Datenfusion und -bereitstellung anbieten, die nicht statisch konfiguriert sondern zur Laufzeit geändert werden kann (s. Abschnitt 4.1). Im Rahmen der laufenden Arbeiten vermeiden wir zunächst den Aufwand, AUTOSAR in einer mixed-criticality Umgebung einzusetzen bzw. mit einer dynamischen Middleware zu verbinden.

3 Ein datenzentrischer Ansatz für die IKT-Architektur Elektrofahrzeuge

Um die in Kapitel 1 dargestellten Probleme derzeitiger Fahrzeug-E/E-Architekturen durch den Einsatz der in Kapitel 2 vorgestellten, zentralisierten Systemarchitektur zu lösen, wird eine geeignete Middleware benötigt. In diesem Artikel stellen wir einen datenzentrischen Ansatz vor, der einen hohen Grad an Fehlertoleranz, Flexibilität und Erweiterbarkeit bietet. Im Gegensatz zu den aktuell verfolgten Ansätzen, bei denen von verschiedenen Steuergeräten Nachrichten verarbeitet werden, die auf dem Bus anliegen, wird bei dem hier vorgestellten Ansatz mit Daten gearbeitet, die ein Abbild des aktuellen Fahrzeugzustands wiederspiegeln.

Um die Verschaltung der Software-Komponenten zu ermitteln geben diese an, welche Daten sie benötigen und welche sie bereitstellen. Eigenschaften wie Latenz und Jitter werden dabei durch Quality of Service (QoS) Parameter beschrieben und fließen in die Berechnung mit ein. Auf Basis dieser Informationen wird schließlich die Verschaltung der Software-Komponenten berechnet. In Abschnitt 3.1 wird die grundlegende Funktion des datenzentrischen Ansatzes eingeführt. Im Anschluss daran wird die im Projekt entwickelte, datenzentrische Middleware Chromosome vorgestellt und der Datenfluss im System erläutert.

3.1 Übersicht der datenzentrischen Architektur

Zur Umsetzung der datenzentrischen Architektur werden vorab verschiedene Datentypen (so genannte Topics) definiert. Beispiele für Topics sind die Fahrzeuggeschwindigkeit, Radgeschwindigkeit und Außentemperatur. Softwarekomponenten kommunizieren miteinander ausschließlich über an Topics gebundene Daten, indem sie diese an die Middleware weitergeben bzw. diese von der Middleware erhalten.

Neben den Topics kann es notwendig sein, die Anforderungen an die Daten noch näher zu beschreiben. Dazu werden Meta-Daten verwendet. Diese beschreiben sowohl Anforderungen an die Daten als auch Garantien. Beispiele für Metadaten sind Ort der Erzeugung, Genauigkeit, Konfidenz und Sicherheitslevel.

Die Ausführung der Anwendungen erfolgt zyklenbasiert (Zykluslänge: 10ms). Dabei werden die Daten zum Beginn des Zyklus von der Middleware in den Arbeitsbereich der in diesem Zyklus startenden SW-Komponenten kopiert und bei Beendigung der Funktion aus logischer Sicht (siehe Ausführungszeiten [9]) wieder in die Middleware zurückkopiert. Ein Zugriff der Funktion auf weitere Daten während der Abarbeitungszeit ist nicht möglich. Neben volatilen Daten, also Daten, die in jedem Zyklus neu erzeugt werden, sollten auch persistente Daten unterstützt werden. Persistente Daten behalten dabei solange ihren Wert, bis ein neuer Wert vorliegt.

Zur Umsetzung dieser Konzepte wird die Middleware Chromosome [8] (XME) als Basis verwendet und um die entsprechenden den Anforderungen für RACE im Zuge des Projektes erweitert.

3.2 Chromosome (XME)

Die Chromosome-Middleware (siehe Abbildung 3) besteht aus mehreren, modular gestalteten Komponenten. Eine Auswahl dieser Komponenten wird in diesem Abschnitt betrachtet.

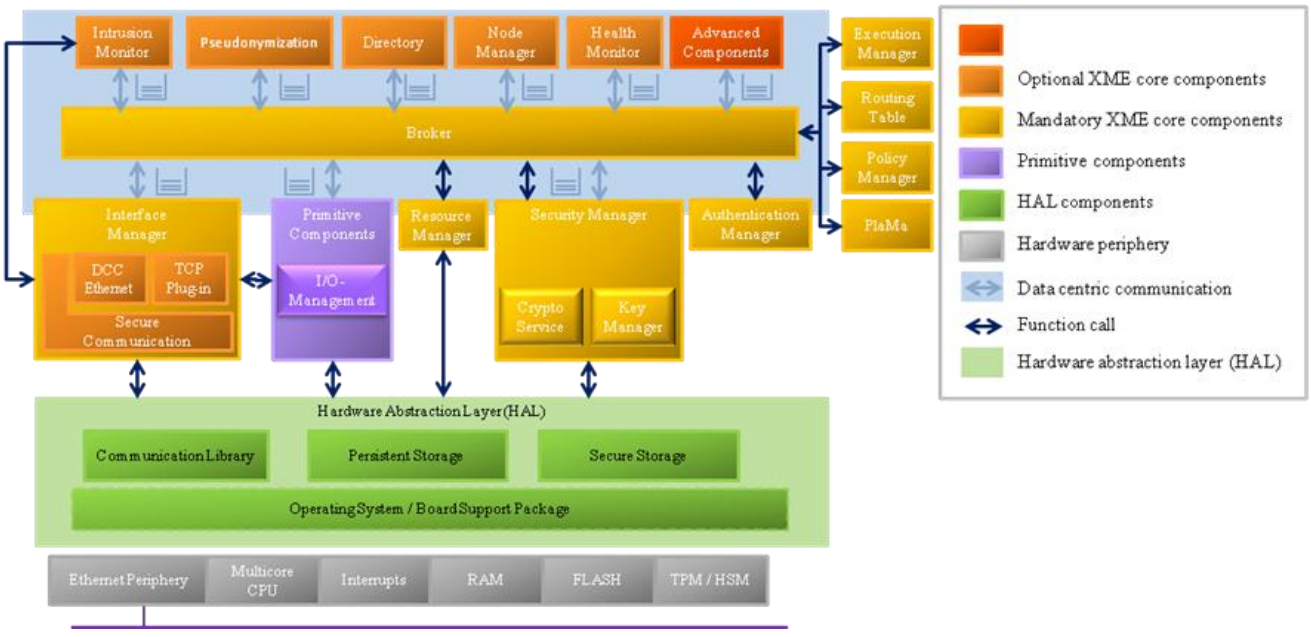

Abbildung 3: Chromosome Stack-Übersicht

Die Hardware-Basis stellen die in Kapitel 2 vorgestellten, gedoppelten Rechner eines DCCs dar. Zur Unterstützung von Anwendungen verschiedener Kritikalitäten wird in RACE ein Betriebssystem mit Virtualisierungsunterstützung verwendet, die Portierbarkeit auf neue Plattformen wird durch einen Hardware Abstraction Layer (HAL) erleichtert. Dieser Kapselt den Zugriff auf die

Hardware bzw. das Betriebssystem und setzt die Arbitrierung beim gleichzeitigen Zugriff auf Ressourcen um.

Die eigentlichen Middleware-Funktionen werden dann im oberen Teil (in der Abbildung hellblau gekennzeichnet) umgesetzt. Die Kommunikation ist im Interface-Manager gekapselt, der, je nach Anforderung der Anwendung, mit Plug-Ins für verschiedene Kommunikationsstandards versehen werden kann. In Standardanwendungen sind dies häufig TCP und UDP, in RACE wird Ethernet (Layer 2) für die sicherheitskritische Kommunikation verwendet. Empfangene Daten werden in der Middleware (Datenbank, siehe nächster Abschnitt) zwischengespeichert und anschließend über den Broker an die einzelnen, lokalen Empfänger verteilt. Dies erlaubt eine vollständige Entkoppelung von Sender (Daten-Produzent) und Empfänger (Daten-Konsument). Die Verschaltung der Komponenten wird dabei vom Directory berechnet und als Konfiguration an die Broker verteilt. Die jeweilige Ausführung der Komponenten (sowohl der Middleware als auch der Anwendung) wird vom Execution Manger angestoßen und überwacht.

Um die Echtzeitfähigkeit des Systems zu garantieren, wird die Ausführung der Funktionen offlinegeplant und online überwacht. Basierend auf Informationen unter anderem zur Worst-Case Execution Time (WCET) können dabei die Komponenten optimal eingeplant werden. Ebenfalls können dadurch Degradationsstrategien festgelegt und hinterlegt werden. Die offline berechnete Allokation der Ressourcen und die Ausführungspläne für die verschiedenen Betriebszustände (incl. Degradationsstufen) sind im Plattform-Management hinterlegt. Zur Laufzeit wird durch das Plattform-Management der aktuelle Ausführungsplan im Execution Manager hinterlegt. Sobald ein Fehler erkannt wird, kann durch das Plattform-Management eine geeignete Alternativkonfiguration im Execution Manager hinterlegt werden.

Für nicht sicherheitskritische Anwendungen ist die Ressourcenplanung für neue, vorher nicht bekannte Anwendungen zur Laufzeit möglich. Die Separation von den sicherheitskritischen Funktionen wird dabei durch Virtualisierung des zugrundeliegenden Systems und der dadurch erreichten Separation sichergestellt. Dies ermöglicht eine wesentlich höhere Flexibilität und somit das nachträgliche einbringen neuer Funktionen in das System (z.B. PnP).

3.3 Logisch zentrale Datenbasis

Um den Anforderungen sicherheitskritischer Anwendungen gerecht zu werden, müssen Daten vor der Verarbeitung in den einzelnen Anwendungen auf Plausibilität geprüft werden. Als zentraler Punkt in XME dient hierzu eine logische, zentrale Datenbank als Datenbasis. Alle von XME bzw. den Anwendungen auf einem Knoten (DCC) verarbeiteten Daten werden zunächst in der logischen Datenbank zwischengespeichert. Zu Beginn eines Zyklus werden die Daten der Anwendung zur Verfügung gestellt. Die Ergebnisse der Anwendung werden nach der Berechnung zum Ende eines Zyklus wieder in die Datenbank geschrieben.

Bei sicherheitskritischen Anwendungen können die Berechnungen einer Anwendung dupliziert auf mehreren Knoten (DCCs) im Netzwerk ausgeführt werden. Dabei werden sowohl die Eingabedaten als auch die Ergebnisse der Berechnungen basierend auf den Ergebnissen in der Datenbank durch das I/O Management verglichen und bewertet.

Neben den Aufgaben im Regelbetrieb ist die Datenbank ebenfalls von zentraler Bedeutung während der Entwicklung und der Systemtests. Dabei werden über die Datenbank synthetische Daten eingespeist bzw. Ergebnisse ausgelesen. Dadurch können künstlich Fehler provoziert bzw. ins System eingespeist und die Reaktion des Systems darauf getestet und aufgezeichnet werden.

3.4 Kontrollfluss

Wie bereits in Abschnitt 3.1 eingeführt, erfolgt die Ausführung von Funktionen in der RACE-Architektur Zyklus-basiert. Je nach Berechnungsaufwand können Anwendungen mindestens einen oder auch mehrere Zyklen zur Berechnung benötigen. Dabei werden der Anwendung die Daten zu Beginn des ersten Zyklus' von der Datenbank zur Verfügung gestellt und am Ende der Berechnung wieder zurück an die Datenbank übertragen. Nach einer optionalen Konsistenzprüfung stehen die Daten dann im nächsten Zyklus für weitere Komponenten zur Verfügung.

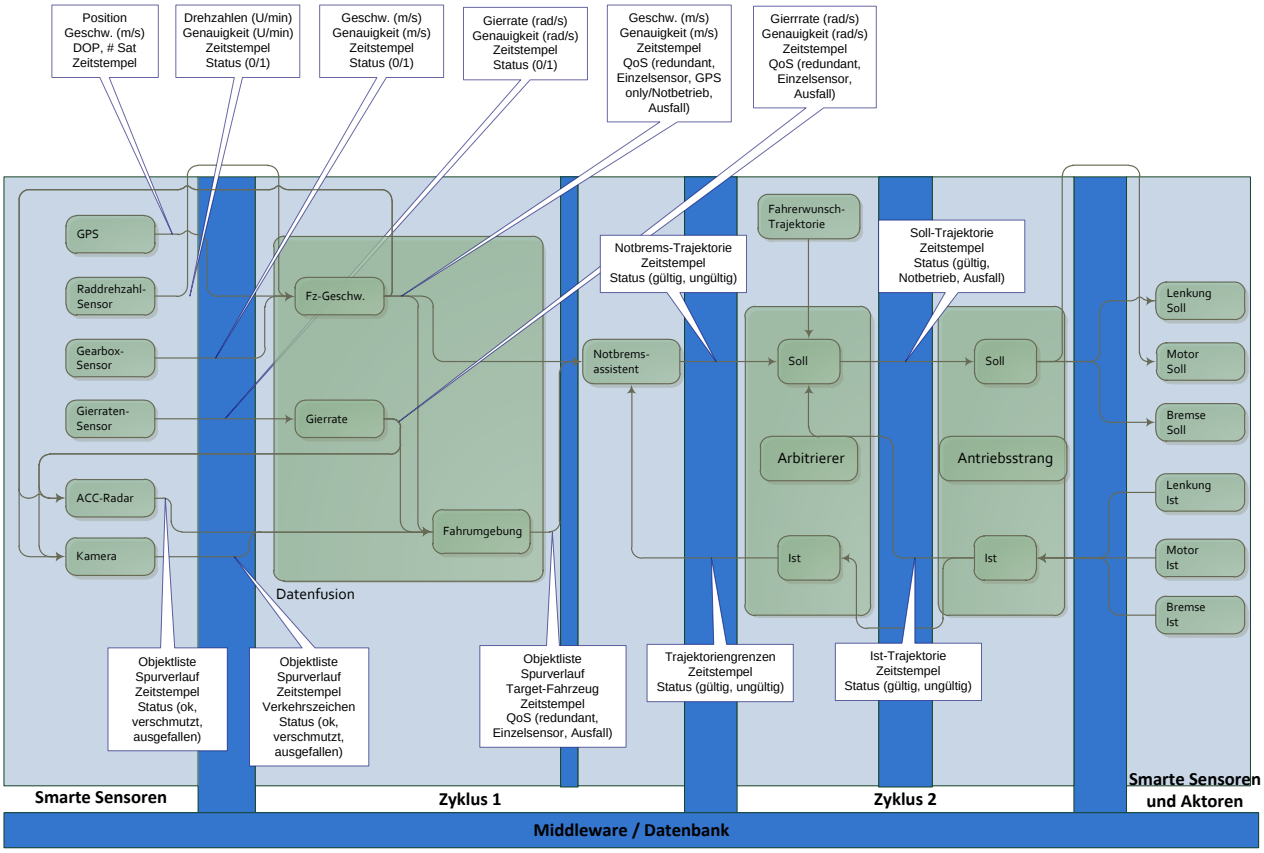

Abbildung 4: Funktionsblöcke der Anwendung Notbremsassistent

Eine beispielhafte Anwendung ist in Abbildung 4 dargestellt. Weder die Sensoren noch die Aktoren sind dediziert für die Funktion Notbremsassistent installiert, noch direkt mit einem dedizierten Steuergerät verbunden, das exakt diese Funktion abbildet. Alle beteiligten Softwarekomponenten werden auf einem Zentralrechner (DCC) ausgeführt.

Zu Beginn werden die Messwerte der Sensoren zuerst über eine Komponente zur Datenfusion vorverarbeitet und in Zusammenhang gesetzt. Die Ergebnisse wie z. B. Objektlisten werden dann an die Software-Komponente des Notbremsassistenten übertragen. Im Arbitrierer werden die Ergebnisse des Notbremsassistenten mit den Eingaben des Fahrers abgeglichen und die Entscheidung über die Fahrstrategie berechnet. Über die Softwarekomponente des Antriebsstrangs werden im Anschluss die einzelnen Stellgrößen für die Aktoren ermittelt und an diese übertragen. In dem gezeigten Anwendungsfall sind die Aktoren zugleich Sensoren. Sie kennen den eigenen Zustand und ermöglichen so der Softwarekomponente für den Antriebsstrang einen Soll / Ist Abgleich.

Durch die Entkoppelung der einzelnen Funktionen und die Verfügbarkeit der Informationen im System wird im Gegensatz zur Realisierung in einem dedizierten Steuergerät die Möglichkeit geschaffen, die Informationen für weitere Funktionen zu nutzen. Dies ermöglicht es den Herstellern z. B. bei bereits ausgelieferten Fahrzeugen Sicherheitsfunktionen nachzurüsten, da nur eine weitere

Software-Komponente installiert werden muss. Für nicht sicherheitskritische Funktionen ist sogar eine Installation von neuen Anwendungen durch den Benutzer während der Fahrt möglich.

4 Neue Funktionen, die durch die Datenzentrik ermöglicht werden

In diesem Kapitel beschreiben wir neue Sekundärfunktionen, die durch die in Kapitel 2 und 3 gezeigten Ansätze ermöglicht werden.

4.1 Nachträgliches Hinzufügen neuer Funktionen (Plug-and-Play (PnP))

Das vorab beschriebene Zentralrechnerkonzept und die Datenzentrik sind eine wesentliche Grundlage, um ein nachträgliches (After-Sale) Hinzufügen von neuen Fahrzeugfunktionen und neuer Fahrzeughardware (z.B. Sensorik) per PnP zu ermöglichen. Bezüglich bereits existierender und neu hinzuzufügender sicherheitskritischer Anwendungen muss das PnP-Konzept besonderen Qualitätsmerkmalen genügen, um die Safety-Eigenschaften nicht negativ zu beeinflussen.

Warum PnP? Eine wesentliche Beschaffenheit von Heimcomputern ist die individuelle nachträgliche Erweiterbarkeit um neue Funktionalitäten in Form von neu installierten Programmen oder hinzufügbarer interner oder externer Hardware. Hierdurch wird es ermöglicht, eine alternde Basisplattform durch Erweiterungen aktuell zuhalten. Dem Kunden wird es zudem durch persönliche Modifikationen erlaubt, sein System individuell zu gestalten. Auch die Entwicklung der letzten Jahre im Mobiltelefonbereich hat gezeigt, dass Kunden individuelle Erweiterungsmöglichkeiten fordern, welche hier in Form des Verkaufs von Anwendungen über online Applikationsmärkte umgesetzt sind. Ein solcher After-Sale Markt ist auch für den Automobilsektor relevant.

Im Automobilbereich ist eine solche Erweiterbarkeit der Fahrzeugfunktionalität ebenfalls wünschenswert. Derzeit ist dieses jedoch nach dem Verkauf kaum möglich. Beim Kauf eines Neuwagens muss sich der Käufer schon während der Bestellung über alle Wünsche bzgl. der erweiterten Ausstattungsoptionen im Klaren sein. Eine nachträgliche Erweiterung ist derzeit i.d.R. aus technischen Gründen kaum möglich. Besonders gilt dies für Fahrzeugfunktionen, die zum Kaufzeitpunkt noch gar nicht verfügbar waren.

Auch aus OEM-Sicht hätte eine Erweiterbarkeit der Fahrzeugfunktionalität enorme Vorteile. So lässt sich der Übergang von einem Fahrzeugmodell zu dessen Nachfolger fließender gestaltet, da eine Erweiterung der Fahrzeugfunktionalität durch das PnP vereinfacht wird. Hierdurch werden auch kürzere Modellintervalle möglich. Auch die Wiederverwendbarkeit bzw. die Aktualisierbarkeit der bereits vorhandenen Software wird erhöht. Gleiches gilt für den Übergang zwischen verschiedenen Fahrzeugmodellen, die auf einem ähnlichen Zentralrechner basieren.

Durch das in diesem Artikel beschriebene PnP-Konzept soll ein Weg aufgezeigt werden, die Probleme derzeitiger Fahrzeuggenerationen zu lösen und eine nachträgliche Erweiterung der Fahrzeugfunktionalität zu ermöglichen, sowohl um neue Software- als auch Hardwarebausteine.

Im Fokus des PnP steht die dynamische Erweiterbarkeit der Menge an Fahrzeugfunktionen und vorhandenen Sensoren und Aktoren. Um das PnP ohne weitere Benutzerinteraktion autonom durchzuführen, ist eine Schlüsselvoraussetzung die Möglichkeit der dynamischen Selbst-Konfiguration des Fahrzeugs. Das Vorgehen hierbei muss Safety-Anforderungen erfüllen (siehe auch [1] und [4]) und zudem durch geeignete Security-Mechanismen abgesichert sein (siehe Kapitel 4.3). Um die Erweiterbarkeit zu gewährleisten sind zudem standardisierte Schnittstellen notwendig.

Während des PnP-Vorganges muss abgesichert werden, dass eine neue Funktion die vorhandenen Funktionen nicht durch Seiteneffekte beeinflusst. Besonders betrifft dies das Scheduling sowie die

Buskommunikation, aber auch den Zugriff auf Aktoren. Ein Mittel ist hierbei unterschiedliche Arten von Funktionen in voneinander entkoppelten Partitionen zu halten. Die Partitionierung kann anhand verschiedener Kriterien erfolgen, z. B. anhand verschiedener Sicherheitsstufen.

In unserem Konzept findet das PnP in der Regel in einem speziellen Wartungsmodus statt, teilweise aber auch im normalen Fahrzeugbetrieb (in einem reduzierten Umfang).

Wir unterscheiden:

1.) PnP im normalen Fahrbetrieb
2.) PnP im Wartungsmodus / beim Systemstart

PnP im normalen Fahrbetrieb:

Aus Safety-Gründen ist das PnP im Fahrbetrieb nur sehr eingeschränkt möglich. Zum einen ist kein Hinzufügen von Hardwarekomponenten (z.B. Sensoren und Aktoren) möglich. Zum anderen ist das Hinzufügen von neuen Softwarefunktionen in den Zentralrechner in der Form eingeschränkt, dass nur freie Ressourcen, die zuvor speziell für das PnP vorreserviert wurden, für neue Funktionen zur Verfügung gestellt werden können. Ressourcen von bereits vorhandenen Funktionen bleiben hiervon unangetastet. Bezüglich der Fahrzeugkonfiguration handelt es sich hierbei also um eine rein additive Ergänzung der Konfiguration, ohne bestehende Konfigurationsteile zu verändern.

Bei diesem rein additiven Vorgehen kann es jedoch zu der Situation kommen, dass der Verschnitt der freien Ressourcen auf den verschiedenen Kontrollrechnern im Zentralrechner so ungünstig ist, dass die Ressourcen nicht mehr ausreichen um eine neue Funktion hinzuzufügen, obwohl die Summe der freien Ressourcen sehr wohl ausreichen würde. In diesem Fall wird im derzeitigen Entwicklungsstadium unseres Konzeptes ein Neustart im Wartungsmodus des Systems notwendig. Hierbei kann eine Rekonfiguration stattfinden, bei der auch bereits bestehende Teile der Konfiguration verändert werden können, um den Verschnitt so zu optimieren, dass das Hinzufügen der Funktion möglich wird (siehe auch „PnP im Wartungsmodus“). Sind insgesamt dennoch nicht genug Ressourcen vorhanden, so wird die neue Funktion entweder abgelehnt, oder eine vorhandene Funktion mit niedrigerer Priorität wird entfernt. Zur Auswahl eines geeigneten Kandidaten zur Entfernung ist ggfls. eine Benutzerinteraktion erforderlich.

Ebenfalls ist beim PnP zu berücksichtigen, dass sich das Fahrzeug in verschiedenen Betriebsmodi befinden kann. Eine Fahrzeugfunktion kann hierbei so konfiguriert werden, dass sie nur in bestimmten Fahrzeugmodi aktiv sein soll. Bezüglich der Selbst-Konfiguration des Fahrzeuges während des PnP bedeutet dies, dass eine Konfigurationsinstanz für jeden Fahrzeugmodus berechnet werden muss.

PnP im Wartungsmodus:

Im Wartungsmodus ist es möglich, bestehende Teile der Systemkonfiguration anzupassen. So kann hier unter anderem das Deployment von Funktionen auf die Kontrollrechner geändert werden, oder auch die Vergabe von Speicher- und Rechenressourcen, oder auch die Netzwerkkonfiguration. Dieses erlaubt die Migration von Funktionen zwischen Kontrollrechnern, um die Systemkonfiguration zu optimieren.

Im Wartungsmodus kann das System auch um neue Hardwarekomponenten ergänzt werden, die automatisch erkannt und eingebunden werden. Zudem können hier Funktionen hinzugefügt, konfiguriert und aktiviert werden, die während des Fahrbetriebs nicht in die Konfiguration eingebunden werden konnten. Solche Funktionen werden im Fahrbetrieb in einem speziellen Funktionsspeicher abgelegt und bei der Initialisierung im Wartungsmodus automatisch erkannt.

Bei der Initialisierung wird zunächst überprüft, ob neue Hardwaremodule hinzugefügt wurden oder ob welche entfernt wurden. Nachdem alle Hardwaremodule erkannt, auf Konformität geprüft und konfiguriert wurden, werden die Softwarefunktionen initialisiert. Es wird eine Minimalkonfiguration von Funktionen und Hardware geprüft (beispielsweise bestehend aus Grundfunktionen wie lenken, bremsen und beschleunigen), ohne die das Fahrzeug nicht als Fahrbereit klassifiziert wird. Andere Funktionen sind dagegen optional (beispielsweise Ultraschallsensoren für die Einparkhilfe sowie die Verarbeitungsfunktion hierzu).

4.2 Redundanz und Safety

Die SW-basierte Integration von Funktionen oberhalb der datenorientierten Middleware erfordert weitere Maßnahmen, wenn es sich um sicherheitskritische Funktionen handelt. Die in Kapitel 2 beschriebene Redundanz der zentralen DCCs kann zur Fehlererkennung und Maskierung genutzt werden, aber die SW-Funktionen müssen im Normalfall auf diese Redundanz angepasst werden. Ein Ziel der Middleware ist es, die Applikationsentwicklung von den Sicherheitsmechanismen der DCC-Hardware-Überwachung, -Umschaltung und Degradation zu trennen, damit die SW-Entwicklung sich auf die Funktionalität und nicht auf die Eigenheiten der DCC konzentrieren kann (horizontale Schichtung.

Die „generische“, funktionsunabhängige Safety bietet im Wesentlichen Fehlerursachenbereich eindeutig zu erkennen und das Eindringen von Fehlern darin zu verhindern [4]. Ein DCC bildet als Rechnerpaar einen solchen Bereich. Beide enthaltene Rechner empfangen und senden im fehlerfreien Fall die gleichen Daten für ASIL-eingestufte Funktionen. Das sog. IO-Management prüft eingehende Daten auf Konsistenz, bevor sie den Applikationen über die MW weitergeleitet werden. Gleiches gilt für ausgehende Daten. Fehler werden nach außen gemeldet bzw. sind eindeutig von außen erkennbar, da auch die Ereignisse doppelt gesendet werden. Dies sichert die Datenkonsistenz (es werden keine fehlerhaften Daten verarbeitet).

Im Falle von Inkonsistenzen wird dieser Fehler dem *Plattform-Management* gemeldet. Dies ist eine auf allen DCCs aktive SW-Komponente, die Aufbau und Konfiguration des Systems sowie mögliche Degradationsstufen kennt. Fehlerindikatoren aus den Applikationen sowie o.g. Integritätsfehler werden hier behandelt. Reaktionsmöglichkeiten umfassen: DCC-Umschaltung auf Slaves und die Abschaltung einzelner Applikationen. Das Plattform-Management sichert dadurch Aktionskonsistenz (die Zentralrechner führen die gleichen Applikationen aus).

Der zyklische Ablauf der Konsistenzsicherung (10ms Zyklen) erlaubt Fehlererkennung und Umschaltung auf einen bereits aktiven (hot-standby) Slave-DCC innerhalb einer Toleranzzeit von 50ms. Auf diesem Wege stellt die Middleware eine fehlersichere Ablaufumgebung für Applikationen zur Verfügung, die auch ASIL-D fail-operational Anforderungen genügt. Diese Sicherung der DCCs enthebt natürlich die Applikationsentwicklung nicht von dem Zwang, nach den Anforderungen der jeweiligen Kritikalitätseinstufung (ASIL-Level) zu entwickeln.

4.3 Security

Security spielt in Kraftfahrzeugen bereits heute eine wesentliche Rolle, um absichtliche Angriffe abzuwehren. Wesentliche Security-Funktionalitäten betreffen die Wegfahrsperre und Fahrzeugschlüssel, korrekter Kilometerstand, zugangsgeschützter Wartungs- und Diagnosezugang einschließlich Feature-Freischaltung und Software-Update („Flashen“) ebenso wie ein Schutz der Fahrzeug-externen Kommunikation mit Backend-Diensten, mit nomadischen Geräten und mit anderen Fahrzeugen (Car-2-X-Kommunikation). Elektrofahrzeuge werden außerdem kryptographische Security-Features für einen Manipulationsschutz des Ladeprotokolls sowie für die Unterstützung von Plug-and-Charge realisieren [11]. Diese Security-Features sind teilweise in Hardware realisiert, um die Performance bzw. die Robustheit der Implementierung zu erhöhen.

Auch in der neuen Systemarchitektur müssen diese bekannten Security-Funktionen robust realisierbar sein. Der in diesem Artikel beschrieben Ansatz für die Fahrzeug-Systemarchitektur erfordert jedoch darüber hinausgehende, spezifische Security-Funktionalitäten. Die wesentlichen Treiber für Security sind dabei das Zusammenführen unterschiedlicher Arten von Funktionen auf einem Zentralrechner sowie die Erweiterbarkeit durch PnP um neue Software-Funktionen wie auch um neue Hardware-Komponenten (Sensoren, Aktoren).

1. *Zusammenführen von unterschiedlich kritischen Funktionen:* Es werden unterschiedlich kritische Funktionen in einer gemeinsamen, verteilten Ausführungsumgebung realisiert. Die Applikationen sind bezüglich ihrer Safety-Anforderung, ihrer Echtzeit-Anforderungen sowie ihrer eigenen Security-Anforderungen unterschiedlich kritisch. Diese Funktionen müssen voneinander logisch separiert werden, um eine gegenseitige Beeinflussung auch bei Ausführung in einer gemeinsamen Ausführungsumgebung zu verhindern.

2. *Erweiterbarkeit (PnP):* Es muss ermittelt werden, ob eine gewünschte PnP-Operation zulässig ist (Freigabe entsprechend Fahrzeug-Security-Policy, Lizensierung/Know-How-Schutz, für PnP-Operation berechtigter Nutzer), sodass nach einer PnP-Operation eine zulässige Konfiguration vorliegt. Bei einer PnP-Operation müssen die Mechanismen zur Separierung abhängig von den ermittelten Attributen konfiguriert werden. Mit dem Fahrzeugbus direkt dürfen nur vertrauenswürdige Komponenten direkt verbunden werden. Andere Komponenten dürfen nur eingeschränkt Zugriff auf den Fahrzeugbus erhalten.

Weitere Anforderungen an das Design der Security-Lösung kommen aus dem Realisierungs- und Anwendungsumfeld. Wie bereits in vorherigen Kapiteln erläutert, wird die für Safety erforderliche hohe Verfügbarkeit durch redundante Rechner und redundante Kommunikation realisiert. Die Security-Lösung muss daher eine redundante Berechnung von kryptographischen Operationen, eine redundante Übertragung und ein Failover zwischen redundanten Rechnern unterstützen, ohne dass dadurch die Security selbst gefährdet wird. Außerdem ist im Fahrbetrieb ein „fail-operational“ Verhalten erforderlich, sodass auch bei detektierten Security-Vorfällen ein einfaches Abweisen nicht immer eine angemessene Reaktion darstellt.

Im Folgenden werden die konzeptionellen Lösungsbausteine beschrieben, und das Realisierungskonzept wird skizziert.

4.3.1 Security-Lösungsbausteine

Dieser Abschnitt gibt einen Überblick über erforderliche, für diese Architektur spezifische Security-Lösungsbausteine:

- Separierung von Funktionsdomänen: Zwischen unterschiedlichen Funktionsdomäne (z.B. Safety, Body, Komfort, Vehicle Security, Infotainment) wird durch eine Partitionierung die Rückwirkungsfreiheit erreicht. Auch bei einer Fehlfunktion oder einer erfolgreichen Manipulation eines offeneren Funktionsbereichs ist dadurch sichergestellt, dass die kritische Funktionalität nicht beeinträchtigt wird.
- Separierung von Applikationen: Einzelne Applikationen werden voneinander isoliert, sodass eine Beeinflussung durch eine andere Applikation nur über vorgesehene, zugelassene Datenpfade möglich ist, d.h. über berechtigte Zugriffe auf die Signaldatenbank. Die Applikationen sind außerdem von der Ausführungsumgebung RTE isoliert, sodass eine Applikation nicht die interne Funktion der RTE manipulieren kann. Zugriffe auf Sensoren/Aktoren sind nur indirekt über die Signaldatenbank möglich.
- Zugriffskontrolle auf Signaldatenbank: Eine Applikation kann auf Einträge der Signaldatenbank nur zugreifen, soweit sie dazu berechtigt ist.

- Eine Komponente kann nur auf Einträge der Signaldatenbank zugreifen, soweit sie dazu berechtigt ist. Nur vertrauenswürdige Komponenten dürfen direkt mit dem Fahrzeugbus verbunden sein. Andere Komponenten erhalten Zugriff über eine Anschaltkomponente „Vehicle Security Network Guard“. Diese stellt sicher, dass nur zulässige Zugriffe auf den Fahrzeugbus und damit die Signaldatenbank möglich sind.
- Authentisierung einer Software-Applikation. Eine Software-Applikation wird authentisiert, um deren für die PnP-Einbindung verwendeten Attribute korrekt zu ermitteln. Ebenso erfolgt eine Device Authentisierung von Hardware-Komponente, um deren für die PnP-Einbindung verwendeten Attribute korrekt zu ermitteln.
- PnP Security Policy: Bei einem PnP-Vorgang erfolgt eine Prüfung, ob eine PnP Operation zulässig ist. Dabei müssen unterschiedliche Kriterien und Policies unterstützt werden: Die betroffene Fahrzeugfunktionalität (Funktionsdomäne), Lizensierung, der durchführende Nutzer.
- PnP Security Konfiguration: Die vorgesehenen Security-Mechanismen zur Separierung und Zugriffskontrolle müssen bei einer PnP-Operation konfiguriert werden.

Eine robuste Implementierung dieser Security-Features in der RTE kann durch weitere Security-Maßnahmen unterstützt werden. Wesentliche Aspekte hierbei betreffen die Schlüsselspeicherung, z.B. in einem Hardware Secure Element, eine robuste Implementierung von kryptographischen Algorithmen (Seitenkanalresistenz, Fehlerresistenz), ein Security-Hypervisor, ein sicheres Booten, Kommunikationssicherheit auf dem Fahrzeugbus und die Detektion von Manipulationen. Im Fehlerfall sind durch entsprechende Log-Einträge im Fehlerspeicher die Ursache und die Verantwortlichkeit ermittelbar.

4.3.2 Realisierungskonzept Systemarchitektur

Die RACE-spezifischen Security-Funktionen werden durch Security-Module des Runtime Environment realisiert. Für die Erweiterbarkeit (PnP-Manager) benötigte Security-Module sind:

- Device Authentication Module: Authentisierung einer Hardware-Komponente
- Application Authentication Module: Authentisierung einer Software-Applikation
- PnP Security-Policy Manager: Prüfen einer PnP-Operation auf Zulässigkeit
- Access Policy Provider: Berechtigungen bei einem PnP-Vorgang automatisch erzeugen.
- Access Policy Configurator: Berechtigungen auf Enforcement-Komponente konfigurieren.

Für die Durchsetzung der Separierung zur Laufzeit werden folgende Module verwendet:

- Signaldatenbank Access Control: Zugriffskontrolle auf Einträge der Signaldatenbank
- Vehicle Network Access Guard (Real-Time Firewall): Zugriffskontrolle auf den Fahrzeugbus und damit die Signaldatenbank durch eine Hardware-Komponente
- Hypervisor: Angriffs-resistente Separierung von Funktionsbereichen (Partitionierung)

Diese RACE-spezifischen Security-Funktionen verwenden als Basis allgemein bekannte Security-Funktionen zur Schlüsselspeicherung, kryptographische Algorithmen, sicheren Kommunikation, Policy-Prüfungen, Fahrerauthentisierung etc. Weiterhin stellt die RTE einzelnen Applikationen diese Security-Basisfunktionen bereit, um Applikations-spezifische Security-Funktionalität effizient realisieren zu können.

Innerhalb des geschlossenen RTE-Security-Kerns ist ein IT-Security-Schutz nicht zwingend erforderlich. Dabei wird jedoch ein ausreichender physikalischer Schutz der betroffenen Komponenten vorausgesetzt. Die oben beschriebenen Security-Mechanismen schützen vor möglicherweise manipulierten Komponenten, die sich außerhalb des RTE-Security-Kerns befinden, d.h. die Applikatio-

nen und die Hardware-Komponenten. Weitere Security-Funktionen können jedoch einen Beitrag leisten, um den RACE-Security-Kern selbst in Ergänzung zu physikalischen Schutzmaßnahmen angriffsresistent zu realisieren.

4.3.3 Realisierungskonzept Middleware

Die zu Beginn des Kapitels 4.3 formulierten prinzipiellen Ziele der RACE-Security Architektur werden durch den Security Manager und dessen Teilmodule implementiert. Im Folgenden werden einige Module des Security Managers vorgestellt, wie sie in der Abbildung 3 dargestellt werden. Die zur Verfügung gestellten Dienste werden näher betrachtet, die erzeugten Daten und innerer Abläufe erklärt.

Zur Authentifizierung bietet der Security Manager ein *Authentification Module* an. Dieses Modul realisiert Authentifizierungsprozesse bei der Installation und der Aktualisierung von Komponenten. Diese Authentifizierung basiert zum Teil auf dem Austausch und der Überprüfung von Zertifikaten, die durch autorisierte Stellen für die Anwendung ausgestellt wurden. Daneben wird eine Authentifizierung beim Austausch von Daten zwischen verteilten Middlewareinstanzen oder Komponenten durchgeführt. Das Modul benötigt für die Durchführung dieses Dienstes einen kryptographischen Dienst.

Das *Crypto-Service Modul* bietet dem System kryptographische Dienste an. Die für die Berechnungen nötigen Schlüssel werden nicht selbst verwaltet, sondern sind zuvor von einem dafür spezifischen Dienst, dem Key Modul angefordert. Beide Module bildet mit dem Secure Storage eine gesonderte vertrauenswürdige Zone, die es erlaubt direkt auf das verwaltete Schlüsselmaterial zuzugreifen und entsprechend dem erlaubten Zweck zu verwenden. Daneben verwaltet das Modul die Konfigurationseinträge für die im System vorhandenen Verschlüsselungsalgorithmen. Werden neue Algorithmen mittels PnP in das System ein gepflegt, alte oder schwache Algorithmen entfernt oder auf den neuesten Stand gebracht, führt dies zu einer Anpassung der im Modul verwalteten und im Secure Storage Modul hinterlegten Konfiguration.

Die Verwaltung von kryptographischen Schlüsseln übernimmt das *Key Management Module*. Hier können Schlüssel in das System ein gepflegt, entfernt und nach Bedarf angefordert werden. Da direkter Zugriff auf Schlüssel ein Sicherheitsrisiko darstellt, werden die Schlüssel nicht direkt verfügbar gemacht, sondern nur indirekt auf Anforderung bereitgestellt.

Das Speichern von Konfigurationsdateien, Schlüsselmaterial, Zertifikaten und weiteren Middleware immanenten Daten wird durch das *Secure Storage Module* übernommen. Dieser ist selbst verschlüsselt und bietet die Daten nur vorgelagerten Modulen nach Autorisierung über die Schnittstellen des Security Manager Moduls an. Dabei kann das Modul von in Hardware existierender Lösungen (z.B. TPM / HSM) unterstützt werden. Aber das ganze kann auch als reine Softwarelösung angesehen werden, wenn es keine Möglichkeit gibt spezifische Hardwareunterstützung zu nutzen.

Neben den bereits vorgestellten Modulen existieren noch weitere Module, die ihre Dienste der Middleware und den Anwendungen zur Verfügung stellen. Grundsätzlich umfasst das die Dienste *Secure Communication Module* zur Bereitstellung sicherer Kommunikation mit anderen Middlewareinstanzen und Anwendungen, sowie das *Policy Module* zum Prüfen von auszuführenden Aktionen auf deren Zulässigkeit.

Neben den sicheren Verbindungen zwischen den verteilten Middlewareinstanzen baut das *Secure Communication Module* auch die sicheren Verbindungen zwischen einzelnen verteilten Anwendungen auf. Dabei dient dieses Modul als zentrale Anlaufstelle für übergreifende Kommunikation und führt die hierfür nötigen Prozeduren und Modul-Interaktionen transparent durch. Dies schließt die

Überprüfung der Verbindungs-Policies, die Authentifizierung und das konkrete Absichern der Verbindung ein.

Das *Policy Module* dient als zentrale Verwaltungs- und Entscheidungsstelle für die Anwendung von Policies. Module oder auch Anwendungen können hier Entscheidungen über geplante Aktionen oder Parameter für die Aktionen anfragen. Das Enforcement der Policy-Entscheidungen übernimmt hierbei die jeweils anfragende Instanz.

Die Überwachung der korrekten Funktionsweise wird durch den *Intrusion Monitor* realisiert. Dabei wird das Verhalten der Software zentral protokolliert und auf Auffälligkeiten untersucht. Bei einem identifizierten Angriff können lokale Reaktionen eingeleitet oder entsprechende Informationen an eine weitere den Angriff betreffende Middlewareinstanz weitergeleitet werden. Neben der Überwachung von Anwendungen beobachtet der Intrusion Monitor die Kommunikation, die über den Interface Manager verschickt wird. Hierbei arbeitet der Intrusion Monitor mit klassischen Ansätzen um schädlichen Datenverkehr zu erkennen und geeignete Gegenmaßnahmen einzuleiten.

Das *Pseudonymization Module* verändert fahrzeugbezogene Daten derart, dass diese nicht mehr dem Fahrzeug und seinem Halter zugeordnet werden können. Sollen Daten mit der Außenwelt ausgetauscht werden, müssen alle Fahrzeugbeziehungen zuerst vom Modul durch ein Pseudonym ersetzt werden. Dies soll verhindern, dass Fahrzeuginformationen aussagekräftig gesammelt und zum Nutzen dritter ausgewertet werden können. Auch verwaltet dieses Modul die Zugriffsrechte auf einzelne fahrzeugbezogene und halterbezogene Daten.

4.4 Weitere Qualitätseigenschaften

Die datenzentrische Middleware unterstützt die *Übertragbarkeit* von Datenproduzenten und Datenkonsumenten. Sie sind voneinander entkoppelt und somit wird die nahezu beliebige Platzierung von Funktionen auf den DCCs möglich. Die Entkoppelung der Funktionen sowohl untereinander also auch von der Hardware ermöglicht die effiziente, plattformunabhängige Implementierung und somit eine einfache Übertragung auf ein neues Zielsystem. Die Anpassung der Verschaltung erfolgt dabei automatisch durch die Middleware.

Die zentralisierte Datenbank unterstützt die *Testbarkeit* des Systems. Die Ein/Ausgaben der Anwendungen sind darüber verfügbar und die Schnittstellen können sowohl für Unit- wie auch für Integrationstests genutzt werden. Traces und auch Fehlerinjektionen sind über diese Komponente der Middleware leicht möglich. Desweiteren sind die Mechanismen der Middleware selbst leichter testbar, da die Ergebnisse von Konsistenzprüfung, Zeitmessungen, etc. als Output der Middleware über die Datenbasis abfragbar und damit testbar werden.

In Zukunft werden wohl nur die kleinsten ECUs ohne *Multicore-Support* auskommen können. Erfahrung aus der Programmierung großer IT-Systeme hat gezeigt, dass eine datenfluss-zentrierte Programmierung leichter über mehrere Prozessorkerne skaliert als eine Task-synchrone Programmierung. Der vorgestellte Ansatz unterstützt einen solchen Datenfluss und erlaubt zusammen mit der Separierung von Partitionen in der RTE die Kombination mit deterministischen harten Echtzeitaufgaben. Die extrem kleinen Zykluszeiten der Aktoren werden in der vorgestellten Systemarchitektur von den koordinierenden Aufgaben der Zentralrechner getrennt.

Die *Kosten* sind ein wesentlicher Treiber für den automobilen Architekturentwurf. Der vorgestellte Ansatz ist kein Weg, Siliziumfläche oder Stücklisten zu minimieren. Vielmehr zielt er auf die Erweiterbarkeit und Entwicklungsgeschwindigkeit ab, in dem Basismechanismen der Rekonfiguration und Safety in einer Referenzarchitektur so von den Anwendungen entkoppelt werden, dass eine getrennte Anwendungsentwicklung ermöglicht wird.

5 Zusammenfassung

Die vorgestellte datenzentrische Middleware unterstützt die SW-basierte Integration von Funktionen. Über die bereitgestellten Daten lassen sich Funktionen kombinieren, die von unterschiedlichen Zulieferern entwickelt werden. Automatische Rekonfigurationsverfahren erlauben das nachträgliche Einbringen von Funktionen, und dies unterstützt auch verschiedenen Entwicklungszyklen für einzelne Funktionen. Die entworfene Systemarchitektur erlaubt eine Kombination mit Safety-Mechanismen, die Fehlererkennungsraten bis zu ASIL-D aufweisen können.

Das vorgestellt Konzept wird im Rahmen des BMWi Förderprojektes „Robust and Reliable Automotive Computing Environment for Future eCars“ (RACE) umgesetzt [3]. Innerhalb des Projekts wird die Middleware ausgebaut und verfeinert. Ein wesentliches Ziel ist es, sowohl die Erweiterbarkeit der datenorientierten Integration sowie die mögliche Zertifizierbarkeit nach ASIL-D aufzuzeigen. Es wird anhand von zwei Versuchsfahrzeugen praktisch erprobt. Die gewonnen Erfahrungen könnten zukünftig mit vorhandenen AUTOSAR-Basisdiensten kombiniert werden und ggf. als Input für eine Erweiterung des Standards dienen; dies ist aber nicht Teil des laufenden Projekts. In diesem Sinne soll RACE aufzeigen, ob dynamische Erweiterbarkeit ein gangbarer Weg in der Automobilindustrie ist.

6 Literatur

[1] M. Armbruster et al., Ethernet meets Safety, 4. Elektronik Automotive Congress, Feb. 2012

[2] G. Spiegelberg, „Ein Beitrag zur Erhöhung der Verkehrssicherheit und Funktionalität von Fahrzeugen unter Einbindung des Antriebstrangmoduls MOTionX-ACT®“, ISBN 9783898733670

[3] http://www.projekt-race.de

[4] Armbruster, M., Zimmer, E., Lehmann, M., Reichel, R. et al., "Modularisation of Safety & Control for X-By-Wire Multiapplication-Platforms," SAE Int. J. Passeng. Cars - Electron. Electr. Syst. 1(1):8-17, 2009, doi:10.4271/2008-01-0113.

[5] ISO/DIS 26262: - Road vehicles – Functional Safety — Part 1-10

[6] Buckl, Christian; Camek, Alexander; Kainz, Gerd; Simon, Carsten; Mercep, Ljubo; Staehle, Hauke; Knoll, Alois; , "The software car: Building ICT architectures for future electric vehicles," IEEE International Electric Vehicle Conference (IEVC), 2012, pp.1-8, 4-8 March 2012.

[7] http://www.fortiss.org/de/forschung/projekte/elektromobilitaet-ikt-architektur-2030.html

[8] http://chromosome.fortiss.org

[9] Henzinger, T. A.; Horowitz, B. & Kirsch, C. M. Giotto: A time-triggered language for embedded programming Proceedings of the First International Workshop on Embedded Software (EMSOFT), 2001, 166 - 184. http://mtc.epfl.ch/~tah/Publications/giotto.pdf

[10] M. Broy, „Mit welcher Software fährt das Auto der Zukunft?“, ATZ extra, 125 Jahre Automobil, pp. 92-97, April 2011

[11] Rainer Falk, Steffen Fries: Securing the Electric Vehicle Charging Infrastructure – Current status and potential next steps, 27. vdi/VW Gemeinschaftstagung “Automotive Security”, Oct 2011, Berlin, VDI-Berichte 2131, VDI-Verlag Düsseldorf.

[12] SPARC Secure Propulsion using Advanced Redundant Control, FP6, IST-2002-507859.

[13] HAVE-IT, FP7, http://www.haveit-eu.org