Schlussbericht zu Nr. 8.2 NKBF 98

- Schlussbericht AutoKonf –

Zuwendungsempfänger:	**BMW AG, München**
Förderkennzeichen:	**16EMO0205**
Laufzeit:	**01.10.2016 – 31.09.2019**
Vorhabensbezeichnung:	**„AutoKonf - Automatische rekonfigurierbare Aktorikansteuerungen für ausfallsichere automatisierte Fahrfunktionen – Teilprojekt: Anforderungen und Vernetzungskonzept für eine rekonfigurierbare Steuerungsplattform“**

Inhaltsverzeichnis

I. Kurzdarstellung

1. Aufgabenstellung

Das Gesamtprojekt „Automatische rekonfigurierbare Aktorikansteuerungen für ausfallsichere automatisierte Fahrfunktionen – AutoKonf“ zielte auf die Entwicklung eines automatisch rekonfigurierbaren Steuergeräts für den Einsatz in hochautomatisierten Fahrzeugen. Als Beispiel sind die Funktionen Lenkung und Bremse ausgewählt worden. Dazu muss das redundante Steuergerät je nach benötigter Funktion im Fehlerfall automatisch rekonfiguriert werden (Autokonf), um die ausgefallene Funktion zu übernehmen.

Im Teilprojekt „Anforderungen und Vernetzungskonzept für eine rekonfigurierbare Steuerungsplattform“ entwickelte BMW zusammen mit den Partnern ein Rekonfigurations- und Rückfallebenen-Management für die Softwarearchitektur und die Vernetzungskonzepte. Dazu war der Aufbau einer Simulationsumgebung notwendig, um die Auswirkungen der Rekonfigurationszeit auf das Fahrverhalten und die Wahrnehmung des Fahrers zu simulieren. Hieraus wurden Ziele und Konzepte für die technische und funktionale Sicherheit der autonomen Fahrfunktionen abgeleitet. Als beispielhafte Umsetzung hat BMW gemeinsam mit den Partnern eine generische Steuergeräteplattform entwickelt, mit der das Vernetzungskonzept für Brems- und Lenkungsfunktionen darstellbar ist.

2. Voraussetzungen

Neben der Fokussierung auf elektrische Antriebe, sind hochautomatisierte Fahrzeuge ein anhaltender Trend in der Automobilindustrie, dem selbst Internet- und Technologiekonzerne folgen [1] [2]. Die deutsche Regierung betont die Bedeutung des automatisierten Fahrens für den Wirtschaftsstandort Deutschland auch durch verschiedene Strategiepapiere [3] [4].
Die Einführung hochautomatisierter Fahrfunktionen wird die E/E-Architektur von Fahrzeugen stark verändern. Unter anderem wird eine zuverlässige Infrastruktur unverzichtbar sein. Noch ist der Fahrer zu jedem Zeitpunkt für sein Fahrzeug verantwortlich. Er ist sozusagen das Backup für eventuelle Funktionsausfälle. Diese Option entfällt, wenn sich der Fahrer mit der Einführung hochautomatisierter Fahrfunktionen beliebig beschäftigen kann. Tatsächlich müssen für eine hohe Akzeptanz automatisierter Fahrzeuge Sicherheits- und Qualitätsansprüche von Beginn an erfüllt sein, was auch eine Redundanz zahlreicher Komponenten bedingt. Wegen des knappen Bauraums im Fahrzeug und limitierender Kostenfaktoren können aber nicht alle neuen Fahrzeugkomponenten redundant geplant werden.
Aus psychologischen Untersuchungen geht hervor, dass ein Fahrer etwa 15 Sekunden benötigt, um seine Beschäftigung zu beenden und die Kontrolle über das Fahrzeug wieder zu übernehmen [5] [6] [7]. Ein Fahrzeug sollte daher mindestens 40 Sekunden und bis zu mehreren Minuten nach einem Fehler sicher arbeiten. Dies gibt dem Fahrer Zeit, um die Kontrolle des Fahrzeugs zu übernehmen. Falls er dazu nicht in der Lage ist, muss sich das Fahrzeug selbstständig in einen sicheren Zustand überführen. Beispiele für solche Fehlerszenarien sind falsche, verzögerte oder fehlende Informationen, Ausfall einer Komponente oder Verlust der elektrischen Energieversorgung.
Um im autonomen Fahrmodus im Fehlerfall einen sicheren Zustand erreichen zu können, sind Lenkung und Bremse unabkömmlich. Damit kann das Fahrzeug die Fahrspur halten, im Idealfall den Standstreifen ansteuern und letztlich zum Stillstand kommen. Die Zuverlässigkeit

aktueller E/E-Architekturen reicht für diese sicherheitskritische Aufgabe allerdings nicht aus. Es sind Neuentwicklungen von Hard- und Software nötig, um ein fehlertolerantes System zu kreieren, das Fehler erkennt, isoliert und adäquat auf sie reagiert.

Das Konsortium hat im Projekt AutoKonf daher eine intelligente Redundanz für Lenkung und Bremse umgesetzt, indem es ein rekonfigurierbares Steuergerät für beide Fahrfunktionen entwickelte. Dies umfasste sowohl das Design neuartiger Hard- und Software inklusive Aufbau der Musterkomponenten, als auch deren Validierung in einem Prüfstand.

Das BMW-Teilprojekt „Anforderungen und Vernetzungskonzept für eine rekonfigurierbare Steuerungsplattform“ kümmerte sich in Hinblick auf das Gesamtprojekt um die Gestaltung zukünftiger Steuergeräteplattformen und systemübergreifender Kontrollmechanismen als Basis für die Realisierung hochverfügbarer Funktionen. Dazu zählen unter anderem das Management von Rückfallebenen und das Umschalten aktiver Pfade.
Funktionen können dabei auf einen standardisierten Satz von fail-operational-patterns, -mechanismen und Systemfunktionen zurückgreifen, wodurch funktionsspezifische Mechanismen nicht mehr redundant aufgebaut werden müssen. Das dazu notwendige Rekonfigurations- und Rückfallebenen-Management in der Softwarearchitektur und in den Vernetzungskonzepten wurde gemeinsam von BMW mit den Projektpartnern erarbeitet.
Die beispielhafte Umsetzung erfolgte durch eine generische Steuergeräteplattform, auf der das Vernetzungskonzept für Brems- und Lenkungsfunktionen umgesetzt wurde. Zum Ende des Projekts validierten die Partner die intelligente Redundanz für Lenkung und Bremse auf Basis der entwickelten Steuergeräteplattform am Prüfstand.

3. Planung und Ablauf des Vorhabens

Das Gesamtprojekt AutoKonf gliederte sich in neun aufeinander aufbauende Arbeitspakete (AP1 – AP9). Dabei konnten im Bereich der Komponentenentwicklung die Arbeitspakete AP4 bis AP7 von den Partnern parallel bearbeitet werden, wobei sich die Entwicklungstätigkeiten teilweise gegenseitig beeinflussten. In diesen Fällen wurden die Ergebnisse der parallel laufenden Entwicklungstätigkeiten stetig abgeglichen.

AP	Bezeichnung	Verantwortlicher Partner
AP1	Fahrzeugstabilitätsanforderung an die Chassisrekonfiguration und ihre Infrastruktur	ITK
AP2	Design eines rekonfigurierbaren Systems	ITK
AP3	Ableitung der Komponentenanforderungen	Intedis
AP4	Entwicklung der Chassis ECU	Hella
AP5	Entwicklung des Vernetzungskonzepts	BMW
~~AP6~~	~~Entwicklung einer betriebssicheren Energieversorgung~~	~~Leoni~~
AP7	Entwicklung der rekonfigurierbaren Steckverbindung	IZM-OPH
AP8	Musteraufbau	Intedis
AP9	Systemvalidierung im VeHIL	Intedis

Tabelle 1: Übersicht über alle Arbeitspakete und dafür verantwortliche Partner. AP6 wurde ersatzlos gestrichen, da Leoni sich im März 2017 aus dem Projekt AutoKonf zurückzog.

Die Arbeitspakete wurden gemäß den Arbeitsinhalten in weitere Teilarbeitspakete unterteilt, um die Entwicklungstätigkeiten transparenter darstellen zu können. Eine Übersicht über die

geplanten Teilarbeitspakete sowie die Bearbeitungszeiträume der einzelnen Entwicklungstätigkeiten sind als Balkenplan in Abbildung 1 ersichtlich.

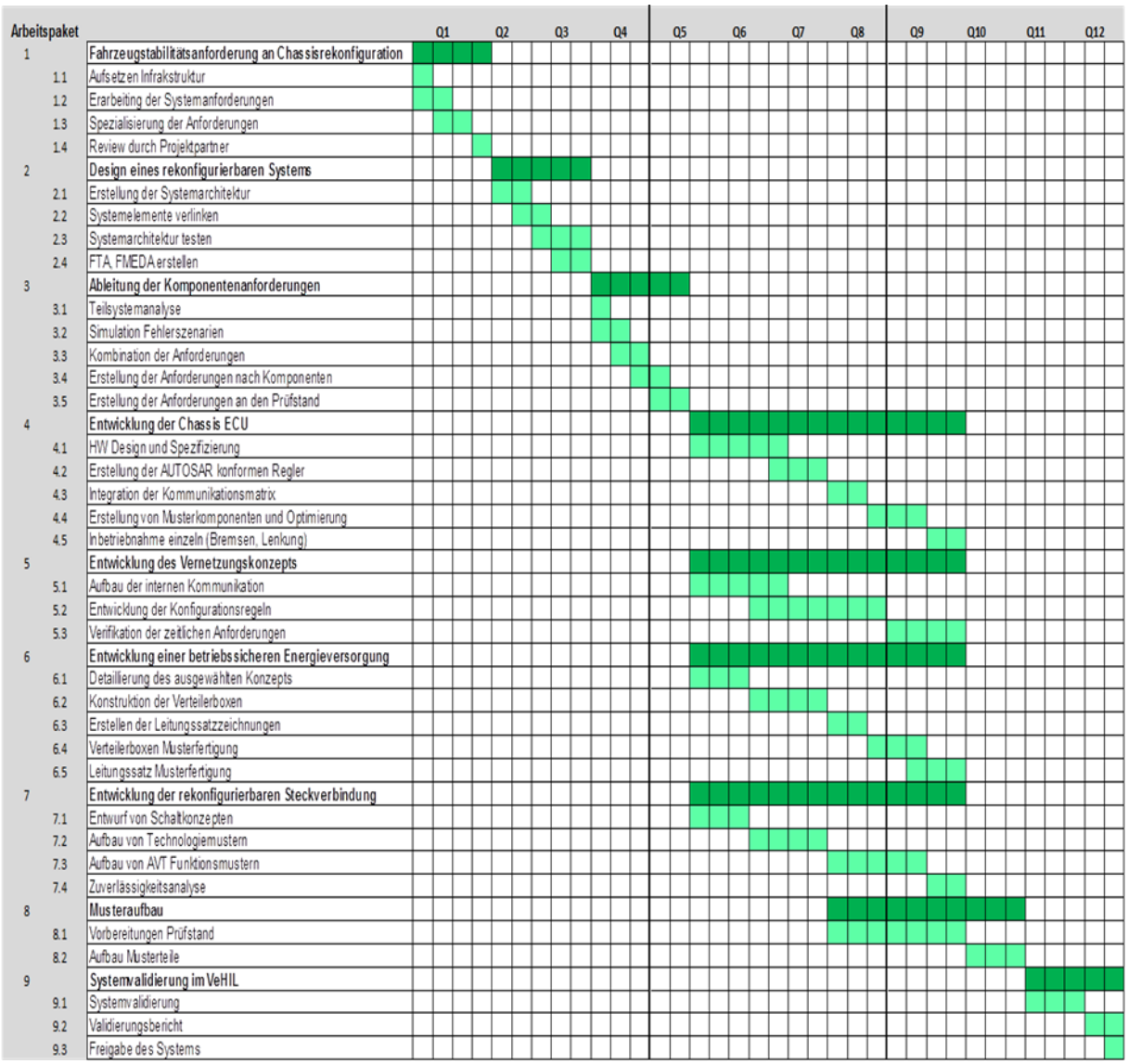

Abbildung 1: Balkenstrukturdiagramm für das Verbundvorhaben AutoKonf

Um die Qualität der Projektergebnisse sicherzustellen, wurden im Gremium verschiedene Meilensteine festgelegt. Durch diese wurden an den neuralgischen Punkten des Projekts Erfolgskontrollen durchgeführt. In Abbildung 2 sind die Meilensteine im zeitlichen Verlauf des Projekts dargestellt, in Tabelle 2 sind die Inhalte und Kriterien der Meilensteine, sowie ihr zeitliches Eintreten festgehalten.

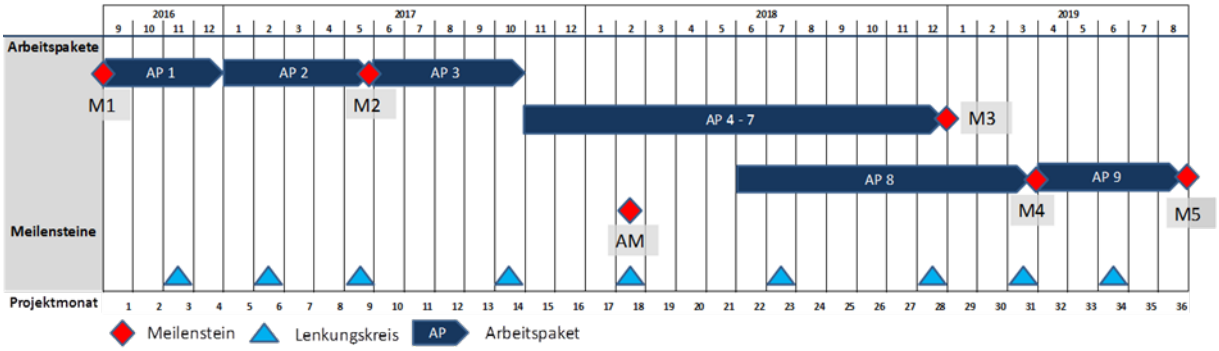

Abbildung 2: Zeitlicher Ablauf der Arbeitspakete und Meilensteine

Meilenstein		Monate nach Projektstart	Kriterien
M1	Kick-Off	0	
M2	System definiert	9	• Freigabe der Systemanforderungen • Ausführbare Systemarchitektur • Bewertung der Systemarchitektur
AM	Abbruchmeilenstein	18	• Technische Machbarkeit • Realisierbarkeit Komponentenanforderungen • Entwicklung der Komponenten & Software
M3	Start der Integrationsphase	28	• Freigabe der Komponenten für Systemintegration
M4	Beginn der Validierungsphase	31	• System bereit zur Validierung • Simulationsmodell angepasst • Fertigstellung des Lastenhefts
M5	Projektende	36	• System gegen Simulation validiert • Anfertigung Abschlussbericht

Tabelle 2: Beschreibung der Projektmeilensteine und Abbruchkriterien für das Projekt AutoKonf

4. Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Das Projekt AutoKonf baut auf einer Reihe von wissenschaftlichen und technischen Vorüberlegungen und Konzepten auf, die aus den Bereichen autonomes Fahren [1] - [7], ausfallsichere Chassis für elektronische Fahrzeugfunktionen [8] [9] [13] [14] [15], redundante Energie- und Datenverteilung in Steuerungssystemen [10] [11] [15], sowie der Modularität und Rekonfiguration von Steuerungssoftware stammen [12] [17].

Dabei wurden im Stand der Wissenschaft und Technik zu Projektbeginn nur jeweils einzelne Aspekte des Vorhabens AutoKonf aufgegriffen. Teilweise stammten die Vorüberlegungen nicht aus dem automobilen Anwendungsbereich. Beispielsweise adaptierten die Forscher fundamentale Elemente der Rekonfiguration von Supercomputern im Projekt, um die komplette Funktions-Rekonfiguration komplexer Komponenten realisieren zu können [17] Dieser Projektaspekt von AutoKonf war zuvor völlig unerforscht und stellt eine wissenschaftliche Innovation und ein Alleinstellungsmerkmal des Projekts dar.

Beim Aufbau der Hard- und Software der einzelnen Komponenten, Leitungen und Schnittstellen setzten die Projektpartner teilweise auf marktübliche Technologien, die jedoch durch ihre projektspezifische Zusammenstellung weit über den Stand der Technik hinausgingen und somit ebenfalls unmittelbar dem Projekt zuzuschreibende Innovationsschritte waren.

5. Zusammenarbeit mit anderen Stellen

Das Forschungsprojekt AutoKonf startete mit den sechs gleichgestellten Partnern

- BMW AG,
- Hella KGaA Hueck & Co.,
- Intedis GmbH & Co. KG,
- ITK-Engineering AG,
- Fraunhofer Institut IZM und
- LEONI Bordnetz-Systeme GmbH,

wobei die Leitung des Gesamtprojekts bei Intedis lag. Die Verantwortlichkeiten der Partner wurden auf die einzelnen Arbeitspakete verteilt, wobei Intedis als Projektkoordinator einen Lenkungskreis zur Seite gestellt bekam, um die gemeinsame Umsetzung der Projektziele sicherzustellen.

Vor Projektbeginn wurden im Konsortium Regeln vereinbart, um den Umgang mit geistigem Eigentum zu definieren: Die Partner brachten benötigtes Hintergrundwissen zu ihren Aktivitäten ein. Außerdem wurden zusätzliche Nebenkenntnisse eingebunden, die während des Projekts gewonnen wurden.

II. Eingehende Darstellung

1. Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele

Als gleichwertiger Projektteilnehmer engagierte sich BMW gemeinsam mit den Projektpartnern an der Entwicklung des Gesamtsystems und brachte dabei die Erfahrung und Anforderungsprofile aus der großseriellen Automobilproduktion in das Projekt ein. Im Teilvorhaben „Anforderungen und Vernetzungskonzept für eine rekonfigurierbare Steuerungsplattform“ lag das Entwicklungsziel von BMW auf der Erforschung einer Software-Architektur und eines Vernetzungskonzepts mit Rekonfigurations- und Rückfallebenen-Management, bei dem die Funktionen durch Umschalten aktiver Pfade auf einen Satz von fail-operational patterns, -mechanismen und Systemfunktionen zurückgreifen können. Dadurch ist es möglich, die Anzahl der redundanten Steuergeräte zu minimieren, indem mehrere Funktionen durch ein einziges redundantes Steuergerät abgesichert werden.
Das Teilprojekt konnte von BMW eigenständig bearbeitet werden, wobei sich die Kernarbeiten auf den Entwicklungen des Vernetzungskonzepts und einer angepassten Simulationsumgebung lagen. Um in AP4 und AP5 die Hauptentwicklungsziele des Teilprojekts durchführen zu können, war die Mitarbeit an den vorangehenden Arbeitspaketen sehr wichtig, da hier die Rahmenbedingungen, Anforderungen und Spezifikationen für das Vernetzungskonzept gelegt wurden.

In **AP1** bestanden die Aufgaben von BMW darin, die Systemanforderungen um einen Katalog möglicher Fahrmanöver, Fehlerszenarien sowie Kombinationen aus beiden zu ergänzen und, unter Berücksichtigung der funktionalen Sicherheit in Anlehnung an die ISO26262 ein parametriertes Fahrzeugmodell für den Einsatz in AP2 zu generieren.
Die Fahrmanöver wurden so gewählt, dass aus ihnen grundlegende Anforderungen an das System und sicherheitsrelevante Zielgrößen abgeleitet werden konnten, z. B. die maximale Fehlertoleranzzeit. Die Szenarien hatten direkten Einfluss auf die Leistungserwartung an das neue System. Zudem ergaben sich aus den Worst-Case-Szenarien die Anforderungen an die Fehlertoleranzzeit.
Es wurden zwei Fahrmanöver festgelegt: Der VDA-Ausweichtest und eine schnelle Geradeausfahrt mit ca. 230 km/h. Der VDA-Ausweichtest bietet den großen Vorteil, dass er genormt ist (ISO 3888-2 (VDA-Spurwechseltest)) und dadurch jederzeit reproduzierbar nachgestellt werden kann (Abbildung 3).
Um die Auswirkung der Rekonfigurationszeit auf das Fahrverhalten sowie die Wahrnehmung des Fahrers anhand vorgegebener Fahrmanöver und Fehlerszenarien bestimmen zu können, wurde ein Simulator aufgebaut, bei dem die Daten des Fahrrechners manipuliert werden konnten. (Abbildungen 4 und 5). Anhand von Probandentests und verschiedener Simulationen konnte ein Richtwert für die maximale Rekonfigurationszeit abgeleitet werden.

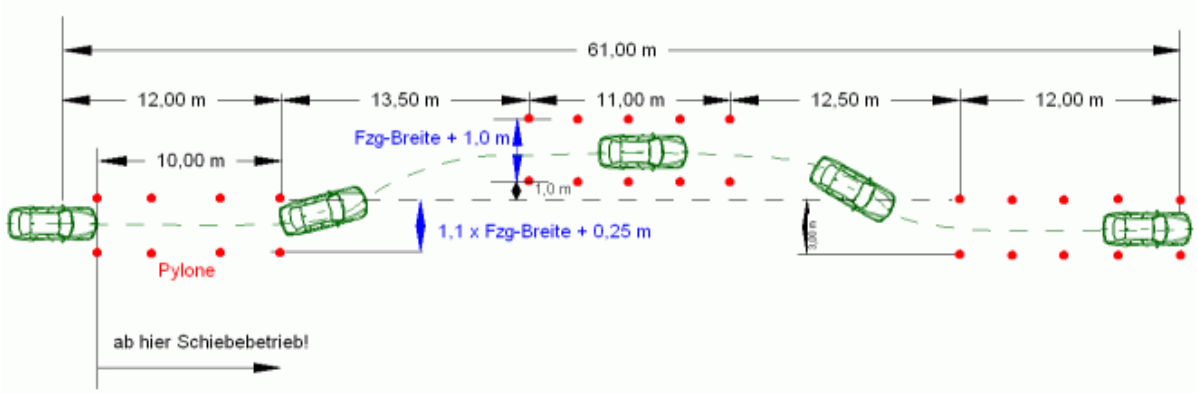

Abbildung 3: VDA-Ausweichtest / VDA-Spurwechseltest nach ISO 3888-2

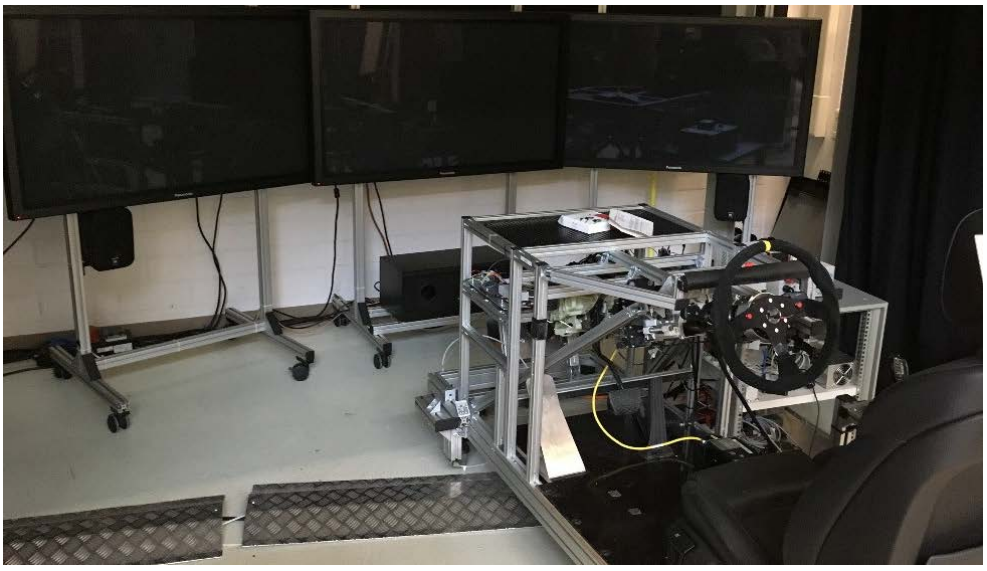

Abbildung 4: Simulationsumgebung zur Ermittlung der maximalen Rekonfigurationszeit

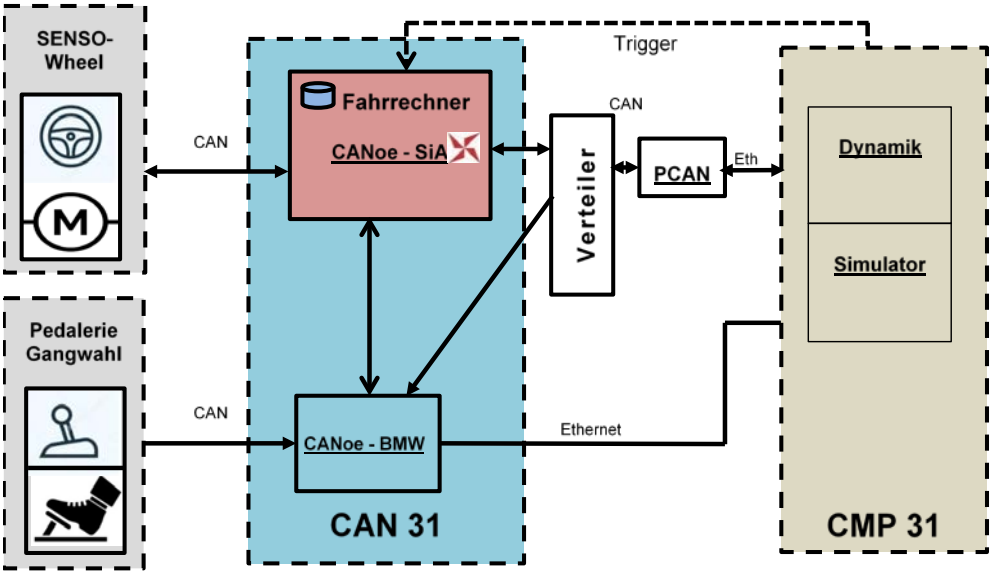

Abbildung 5: schematischer Aufbau des Simulators mit Datenmanipulation

Es wurden verschiedene Probanden-Fahrten und Simulationen mit dem VDA-Ausweichtest und der schnellen Geradeausfahrt durchgeführt, um die maximale Rekonfigurationszeit zu ermitteln. Dabei wurden verschiedene Fehler in der Lenkung simuliert und anhand der Dauer bestimmt, ab welcher Ausfallzeit ein Fehler wahrnehmbar ist, ab welcher Länge ein Fahrer das Fahrzeug nicht mehr kontrollieren kann und in welcher Ausfallzeit des Lenksystems eine sichere Rekonfiguration maximal möglich ist.
In den Testläufen zeigte sich, dass sich eine Fehllenkung schon ab einer Ausfallzeit von 100 ms wahrnehmen lässt. Bei mehr als 200 ms Ausfallzeit konnten die Fahrer das Fahrzeug nicht mehr in allen Situationen abfangen. Als maximal mögliche Rekonfigurationszeit wurden 140 ms ermittelt.
Die Systemanforderungen mitsamt den von BMW ausgearbeiteten Katalogen für Fehler und Fahrmanöver waren daher ein wichtiger Teil des vom Konsortium verabschiedeten Lastenhefts, das ebenso ein Ergebnis von AP1 war, wie die Festlegung eines parametrierten Fahrzeugmodells mit Fahrdynamik- und Lenkungsregelung.

Das Fahrzeugmodell diente im anschließenden **AP2** ─ Design eines rekonfigurierbaren Systems ─ als Basis für die Entwicklungsarbeiten. Das Modell musste in der Lage sein, Fahrmanöver zu fahren, Ausfälle zu simulieren und die Funktionen der Rekonfigurationslogik in definierten Ausfallszenarien zu prüfen. Dafür wurde zunächst eine ausführbare Systemarchitektur erstellt, bestehend aus Hard- und Software sowie systemischen Funktionen. Dabei berücksichtigten die Entwickler alle definierten Anforderungen und achteten speziell auf die funktionale Sicherheit. Ausgehend von im Projektkonsortium diskutierten und bewerteten unterschiedlichen Hardwarearchitekturansätzen, wurde final der in Abbildung 6 dargestellt Aufbau realisiert.
Die Projektpartner bewerteten das Systemverhalten auf Basis des Simulationsmodells und verbesserten das Model in Hinblick auf die Anforderungen. Dabei wurden Sicherheitsanforderungen für alle relevanten Systemebenen der obersten Hierarchieebene erstellt und anhand der Anforderungen verifiziert. Für jede Sicherheitsanforderung wurden dabei auch die entsprechenden Systemspezifikationen erstellt. Die Projektpartner testeten die

ausführbare Systemarchitektur und nutzten die Ergebnisse direkt zur Verbesserung der Systemarchitektur.
Ein auch für das Teilprojekt sehr wichtiger Arbeitsschritt in AP2 war die Erarbeitung der technischen Spezifikationen auf Systemarchitekturebene auf Basis bekannter Sicherheitskonzepte (Funktionssicherheitskonzept (FuSiKo) und Technische Sicherheitskonzepte (TeSiKo), speziell der Fehlerbaumanalyse (engl. Fault Tree Analysis (FTA) und der Fehlermöglichkeits-, Einfluss- und Diagnoseabdeckungsanalyse (engl. Failure Mode and Effects and Diagnostic Analysis (FMEDA)). Die FTA wurde gemeinsam mit allen Projektpartnern durchgeführt und in elektronischer Tabellenform allen Partner zugänglich gemacht. BMW hat das Review des abschließenden Dokuments durchgeführt. Über den Partner Silver Atena von BMW konnte wichtige Entwicklungserfahrung bei sicherheitskritischen E/E-Systeme aus den Bereichen Fahrzeugbau und Avionik in die Ausarbeitung der technischen Spezifikationen einfließen.

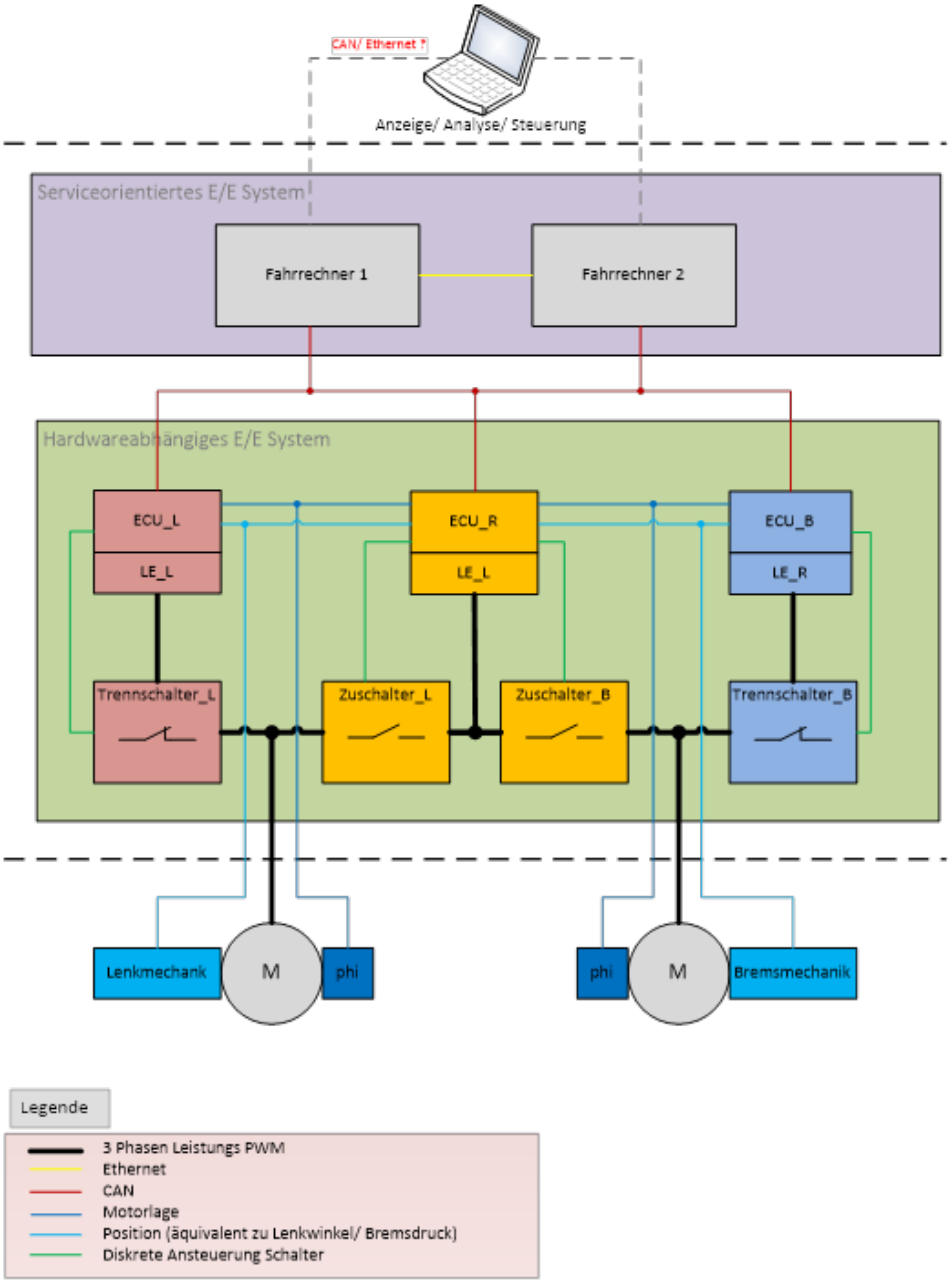

Abbildung 6: Systemkonzept des Projekt AutoKonf inklusive Fahrrechner

Das anschließende **AP3** – Ableitung der Komponentenanforderungen – war das letzte Arbeitspaket, bevor alle Partner parallel zueinander in ihre jeweiligen Entwicklungsphasen starteten. Es umfasste die Ableitung der Systemanforderungen auf die Komponenten.
Zunächst extrahierten die Projektteilnehmer auf Basis des Lastenhefts die Anforderungen an die Teilsysteme und analysierten diese. Zur Erfüllung der Anforderungen entwarfen die Partner verschiedene Konzepte und bauten eine davon für die Simulation auf. Im Fokus standen dabei die Auslegung der Konzepte für die Kommunikation sowie der Leistungsverteilung. Die anschließenden Simulationen der definierten Fehlerszenarien zielten auf eine einheitliche Bewertung der erarbeiteten Konzepte. Neben der Abdeckung der Anforderungen floss auch die jeweilige Umsetzbarkeit in die Bewertung der Konzepte ein. Schließlich wurde ein finales, optimales System evaluiert und festgelegt (Abbildung 7).

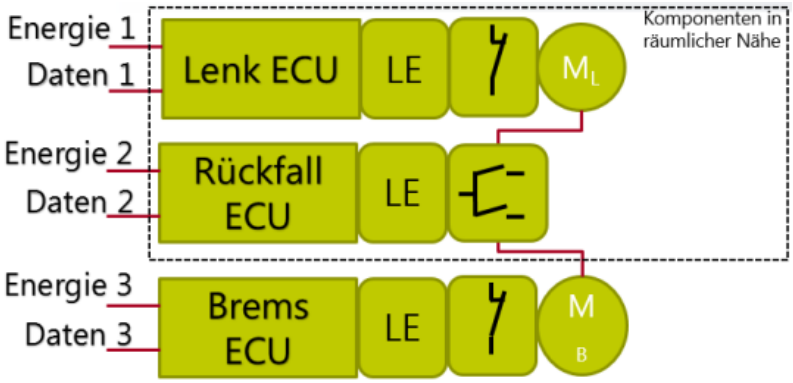

Abbildung 7: Favorisierte Systemarchitektur AutoKonf

Zur Betrachtung der Teilsysteme auf Systemebene kombinierten die Entwickler die Anforderungen, die sowohl die funktionalen Anforderungen an das Verhalten des Algorithmus als auch die Sicherheitsanforderungen an das System umfassten. Daraus konnten die Partner die komponentenspezifischen Entwicklungsparameter ableiten. Notwendig war in diesem Schritt auch die eindeutige Definition der Anforderungen an Energieversorgung, Kommunikation und Rechenleistung der Komponenten, da diese zur Entwicklung der Einzelkomponenten notwendig waren. Zuletzt legten die Partner in AP3 die Prämissen für den Prüfstand fest. Zudem wurden die notwendigen Komponenten und Schnittstellen am Prüfstand abgeglichen und Prämissen zur Durchführung der Testszenarien festgehalten. Der generierte Anforderungskatalog für den Prüfstand umfasst alle relevanten Resultate für den späteren Aufbau des Prüfstands.

Die folgenden Arbeitspakete AP4 bis AP7 umfassten die Entwicklungen der einzelnen Komponenten. Dabei übernahm Hella die Entwicklung der Chassis ECU, bei der das elektronische Steuergerät aufgebaut wurde, das als Kernkomponente die Ansteuerung der Bremsen und des Lenkungssystems gewährleistete (AP4). BMW sorgte für die Entwicklung des Vernetzungskonzepts (AP5), Leoni sollte die betriebssichere Energieversorgung erarbeiten (AP6) und das Fraunhofer-IZM eine rekonfigurierbare Steckverbindung entwickeln (AP7).
Leider hat im März 2017 die Firma Leoni ihre Mitarbeit im Projekt AutoKonf beendet. Damit eine Fortführung des Projektes möglich war, hat sich das Unternehmen aber bereit erklärt, das Projekt mit der Bereitstellung des für die Erstellung des Prüfstandes benötigten Kabelbaums zu unterstützen. Der Ausstieg von Leoni führte dazu, dass die Betrachtung der ausfallsicheren

Energieversorgung im Fahrzeug entfiel. Dies wirkte sich nicht einschränkend auf die Entwicklung der ausfallsicheren Aktorikansteuerung aus, da sie unabhängig von der Betrachtung der Energieversorgung ist und daher wie ursprünglich geplant zwischen den verbleibenden Partnern BMW, Fraunhofer-IZM, Hella, Intedis und ITK stattfinden konnte.

Das von Hella geleitete **AP4** hatte die Entwicklung einer einheitlichen Steuereinheit (ECU) zum Ziel, die sowohl die Funktionalität des Brems- als auch des Lenkungssystems erfüllt, und damit als redundante Steuereinheit eingesetzt werden kann. Als Basis für die HW-Entwicklung kam eine von Hella entwickelte EPS-Plattform zum Einsatz. Diese wurden von BMW und den anderen Partnern gemäß den Anforderungen des Projekts angepasst und erweitert, um Schaltungsanpassungen oder benötigte Schnittstellen zu realisieren. Gerade im Zusammenspiel mit AP5 (Vernetzungskonzept) musste BMW hier die zentrale Abstimmungsarbeit leisten, um die gegenseitige Beeinflussung der Chassis-Entwicklung und des Vernetzungskonzepts bereits in der Designphase des Steuergeräts zu berücksichtigen. Zudem musste BMW die Entwicklungen aus AP4 auch in die Simulationsumgebung integrieren, um dort die gleichen Voraussetzungen und Funktionalität darstellen zu können.
Anhand von System- und Komponentenanforderungen aus vorherigen APs prüften die beteiligten Partner, ob das vorhandene Design ohne Beschränkungen übernommen werden konnte. Auch externe Einflüsse wie Amplitude der elektrischen Ströme, Schwankungen der Bordspannung, Datenrate der Bussysteme und der Einfluss von Störgrößen (elektromagnetische Einstrahlung usw.) wurden beim Design berücksichtigt. Im Designprozess bezogen die Entwickler diese Einflüsse in Ihre Konzepte ein und erstellten mit den passenden Bauteilen ein entsprechendes Schaltungslayout. In regelmäßigen Treffen der Projektpartner wurde das Layout an die Anforderungen des Projekts angepasst und notwendige Schnittstellen abgestimmt. Anschließend konnte mit den AUTOSAR-konformen Reglern für Lenkung und Bremse die Kernfunktionalität des jeweiligen Steuergeräts entwickelt werden.
Ein weiterer Teilschritt in AP4 befasste sich mit der externen Kommunikation zwischen den beiden Steuergeräten, die für BMW eine besondere Relevanz hatte. Um den Datenfluss zu realisieren, wurden die dafür notwendigen Kommunikationsmatrizen festgelegt und offline validiert. Anschließend bauten die Partner mehrere Muster der jeweils entwickelten Komponenten der Steuerungselektronik auf. Diese dienten sowohl als Entwicklungsplattform zur Integration der Regler und Kommunikation, als auch zur Validierung des Systemkonzepts. Als abschließenden Schritt von AP4 nahmen die Entwickler die ECUs zunächst mit einem Brems- bzw. Lenkungssystem einzeln auf entsprechenden elektromechanischen Prüfständen in Betrieb. Die Tests zielten vor allem auf die Qualität der Motorregelung und die Reaktionsgeschwindigkeit.

Im parallel gestarteten **AP5** leitete BMW die Entwicklung eines verlässlichen Vernetzungskonzepts für die interne und externe Kommunikation der verschiedenen Chassis ECUs. Zudem erarbeitete BMW in AP5 die Konfigurationsregeln und verifizierten diese in einer Simulation hinsichtlich ihrer Zeitanforderungen. Die Vernetzung gewährleistet die schnelle und zuverlässige Rekonfigurierbarkeit der eingesetzten ECUs und deren Verbindungen. Dadurch wird die Funktionalität der gesamten Chassis-Infrastruktur sichergestellt. Neben der Auswahl optimaler Leitungen und des passenden Vernetzungskonzepts, sowie der Validierung auf physischer Ebene, spielte auch die logische Ebene eine wichtige Rolle. Außerdem hatten die Inhalte der vorangegangenen Arbeitspakete starken Einfluss auf das Vernetzungskonzept.

Der erste Entwicklungsschritt war die Implementierung der internen Kommunikation innerhalb der Steuergeräte und der Aufbau einer Simulationsumgebung mit Softwareintegrationsplatz bei BMW. Dazu konfigurierten die Entwickler die vorhandene Basissoftware der ECUs gemäß der Anforderungen an die jeweilige Komponente und implementierten die notwendigen Kommunikationstreiber. Diese Aufgabe war von besonderer Bedeutung, da die fertige Konfiguration des Steuergeräts im parallel laufenden AP4 benötigt wurde. Daher erzielten die Entwickler die zeitnahe Fertigstellung und Datenweitergabe an die Projektpartner des anderen Arbeitspakets.
Anschließend begann die Entwicklung des zustandsbasierten Rekonfigurations-Algorithmus, wobei die Kommunikation im Mittelpunkt stand. Unter Berücksichtigung der bisherigen Anforderungen an die Komponenten (AP3), den Konfigurationsregeln und Fehlerantworten (AP1) wurden dazu die Zustandsdiagramme der einzelnen Komponenten aufgebaut. Der ebenenbasierte Ansatz des Algorithmus konnte durch dieses Konzept sehr gut dargestellt werden. Für den angestrebten Zeithorizont wurden relevante Kommunikationstechnologien (OABR, TSN und Optionen der FlexRay-Nachfolge) und Protokolle mit serviceorientierter Architektur betrachtet (SOME/IP) und in Hinblick auf ihre Eignung für das Projekt untersucht.

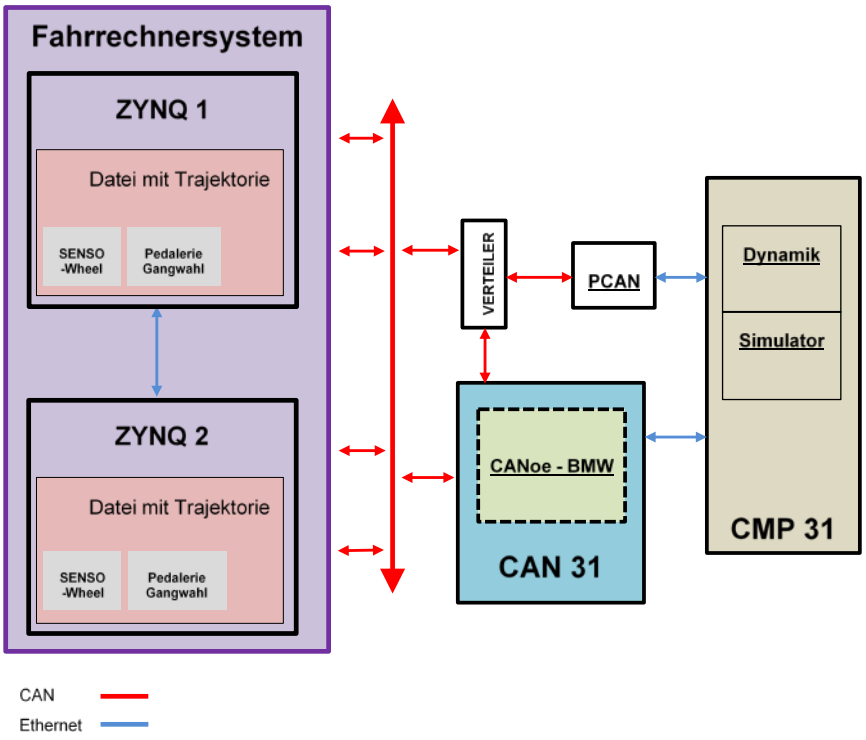

Abbildung 8: Systemaufbau mit zwei ZYNQ-Boards im Fahrrechnersystem mit Abspielmöglichkeit von Trajektorien

Für die Simulationsumgebung wurde die Steuerung von Bremse und Lenkung durch eins der beiden ZYNQ-Boards ersetzt (Abbildung 8). Die Boards haben eine identische Architektur und verfügen jeweils über zwei CAN Schnittstellen zur Anbindung an den Simulator und eine Ethernet-Schnittstelle zur Kommunikation mit dem anderen Board. Die Rolle des jeweiligen Boards (Master oder Backup) hängt von der Variante der Software ab.
Die identischen Architekturen der Boards sind in Abbildung 9 dargestellt. Das Board besteht aus zwei Hauptkomponenten. Die Erweiterte-Simplex Architektur (ESA) stellt die redundante und echtzeitfähige Komponente dar. Der Applikations-Prozessor (APU) stellt hohe Rechenleistung bereit und verwendet ein Linux-basiertes Betriebssystem. Um eine

zuverlässige Kommunikation über CAN zu ermöglichen, werden diese Interfaces von der ESA bedient. Die Berechnung der Trajektorien findet auf der APU statt. Die Kommunikation zwischen den Boards, der Applikation und den Providern findet über das serviceorientierte Kommunikationsprotokoll SOME/IP statt. Die Kommunikation zwischen den Prozessoren (APU, RPU, MicroBlaze und PMU) verwendet ein proprietäres Protokoll.

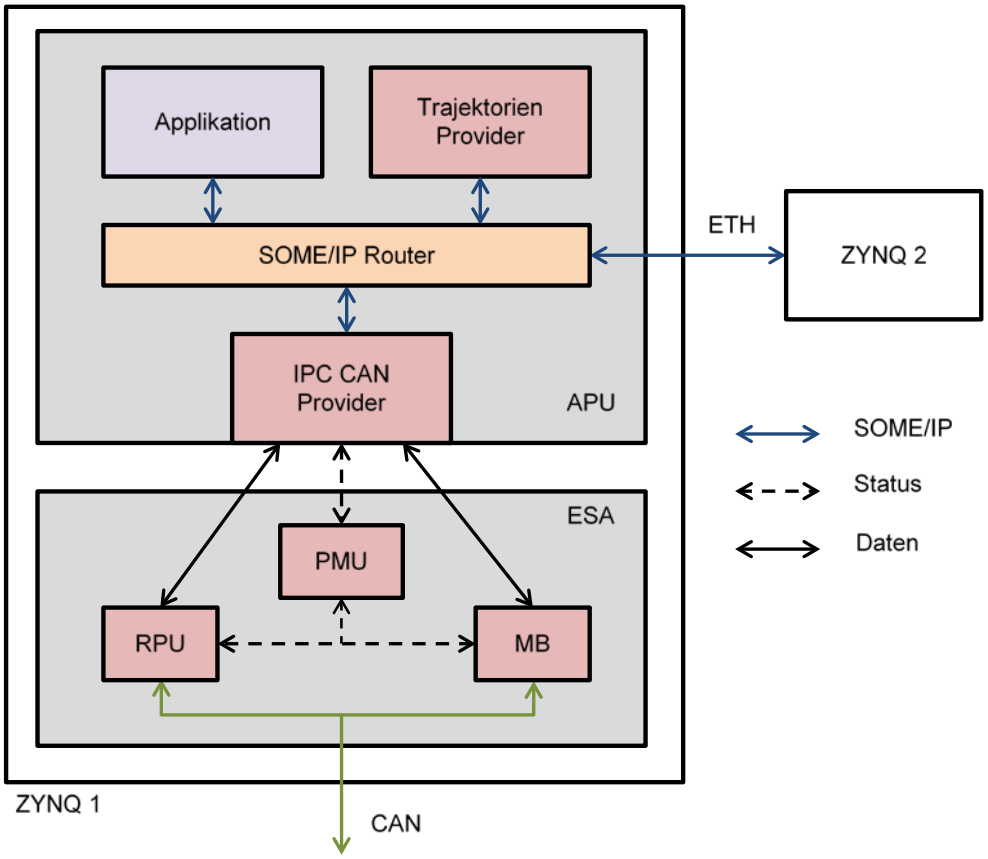

Abbildung 9: Architektur eines ZYNQ-Boards im Projekt AutoKonf

Für jedes Element der Architektur wurde im Folgenden präzise festgelegt, wie die Kommunikation zwischen den einzelnen Bausteinen abläuft, welchen Regeln sie folgt, welche Protokolle zum Einsatz kommen und was für Schnittstellen dabei verwendet werden.
Im Bereich der Software können durch den Trajektorien-Provider auch Fahrten aufgezeichnet, ggf. verändert, und letztlich auch abgespielt werden.
Um das Vernetzungskonzept testen zu können, wurden zwei Simulationsmethoden entwickelt, die die Auswirkung eines Ausfalls von Trajektorien-Provider oder CAN-Provider sowie von einer Fehllenkung beim VDA-Ausweichtest beschreiben. Die zwei Szenarien sind:

1. Fail-operational:
   A. regulärer Betrieb (Referenz)
   B. Ausfall des Real-Time Prozessors
   C. Ausfall des CAN-Interfaces
   D. Ausfall der Trajektorien
2. VDA – Ausweichtest: Abspielen einer Probefahrt mit Fehllenkung mit einem von beiden Fahrrechnern. Es findet kein Providerausfall statt.

Das untersuchte System bietet drei Rückfallebenen:

- Im Falle eines Prozessorfehlers innerhalb der ESA steht ein weiterer Prozessor zur Verfügung.
- Beim Ausfall eines der CAN-Interfaces von einem Fahrrechner, kann die Kommunikation über den zweiten Fahrrechner und Ethernet erfolgen.
- Tritt ein Fehler beim Bereitstellen der Trajektorien auf, übernimmt der Backup-Fahrrechner diese Aufgabe.

Im **regulären Betrieb** (Szenario A) fand eine statische Zeitmessung vom Abspielvorgang im regulären Betrieb statt. Dabei wurde der Provider und der Service lokal auf dem ersten Board des Fahrrechnersystems ausgeführt. Im zweiten Fall wurde der Trajektorien Provider auf dem zweiten ZYNQ-Board, und im dritten wurde der Provider und der Service auf dem zweiten Board ausgeführt.
Es wurden insgesamt drei Fälle mit mehr als 1000 Versuchen simuliert. Im Mittel entsprechen alle Messwerte dem erwarteten Wert von 1 ms. Allerdings traten auch vereinzelt Werte über 2 ms auf. Dies lässt sich darauf zurückführen, dass das SOME//IP kein echtzeitfähiges Protokoll ist. Trotz dieser Abweichung liegt die Verzögerung unterhalb der festgelegten, maximalen Rekonfigurationszeit von 140 ms.

Bei der Simulation eines **Ausfalls des Real-Time-Prozessors** (Szenario B) handelte es sich um eine Zeitmessung im Falle eines Prozessorfehlers innerhalb der ESA, wobei ein weiterer Prozessor zur Verfügung steht (Abbildung 10).

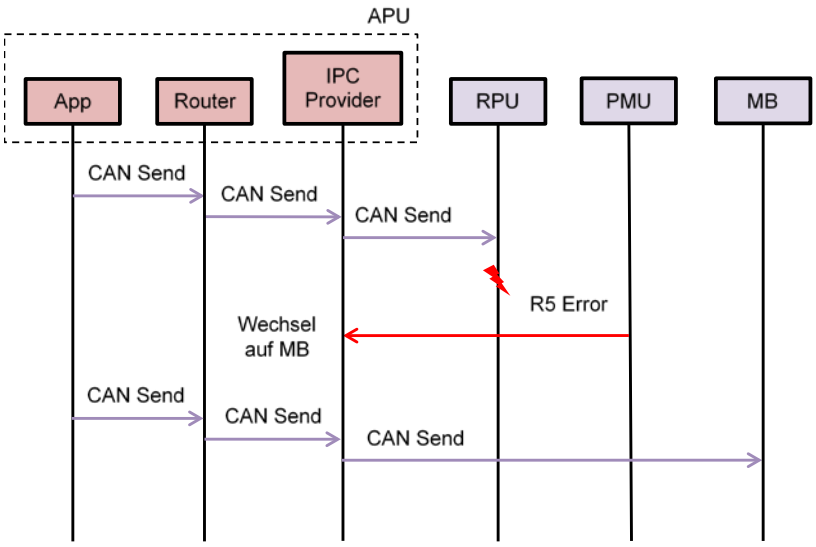

Abbildung 10: Schematische Darstellung eines Ausfalls des Real-Time-Prozessors

Der **Ausfall eines CAN-Interfaces** (Szenario C) stellt eine Zeitmessung beim dynamischen Abspielvorgang im Fail-operational Fall dar. Dabei wurden die Provider zunächst auf einem von zwei Boards ausgeführt. Dann erfolgte ein Umschalten zwischen den Boards bzw. ein Providerausfall. Der Umschaltvorgang erfolgte anhand Service-Discovery beim Ausfall eines

CAN-Interfaces. Der allgemeine Ablauf beim Ausfall des CAN-interfaces ist in der Abbildung 11 dargestellt.

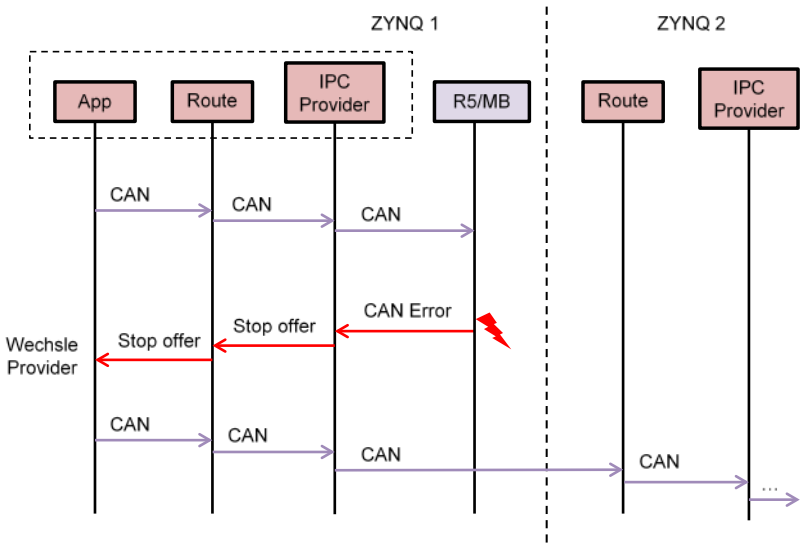

Abbildung 11: Schematische Darstellung eines Ausfalls eines CAN-Interface

Die gemessene Umschaltzeit beträgt 1,342 ms. Da der Vorgang länger als 1 ms gedauert hat, wurde dabei genau ein CAN-Frame verworfen und nicht mehr gesendet.

Beim **Ausfall der Trajektorien** (Szenario D) handelt es sich ebenfalls um eine Zeitmessung beim dynamischen Abspielvorgang im Fail-operational-Fall. Wie schon bei Szenario C wurden die Provider am Anfang auf dem ZYNQ 1 ausgeführt. Auch hier fand ein Umschalten zwischen den Boards bzw. ein Providerausfall statt. In diesem Fall wurde der Trajektorien-Provider mit einem Dateifehler gestört. Der Umschaltvorgang erfolgte anhand Service-Discovery beim Ausfall der Trajektorien. Der allgemeine Ablauf beim Ausfall der Trajektorien wird in Abbildung 12 beschrieben.

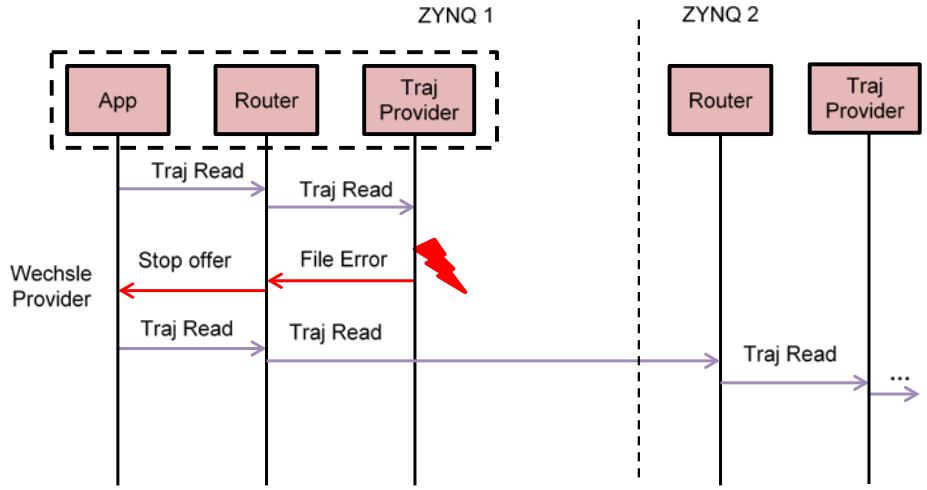

Abbildung 12: Schematische Darstellung des Ausfalls der Trajektorien

Es wurde mehr als 1000 Messreihen durchgeführt, wobei das Umschalten bei allen Messungen maximal 2 ms gedauert hat. Dabei wurde kein CAN-Frame verworfen, sondern

mit einer Verspätung gesendet. Die Messungen haben außerdem ergeben, dass das Umschalten zum neuen Provider bei Ausfällen unterhalb der maximalen Rekonfigurationszeit liegt.

Das Fahrszenario **VDA-Ausweichtest** ist dem Szenario A ähnlich. In diesem Fall wird aber keine Zeitmessung gemacht, sondern eine Positionsmessung des Fahrzeugs, das den VDA-Ausweichtest absolviert. Dabei findet ein Abspielvorgang einer Probefahrt ohne Providerausfall mit einem von beiden Boards statt, das die erzeugte Fahrtrajektorie mit einer in Trace eingebauten Fehllenkung für 140ms bei einer Lenkradgeschwindigkeit von 1°/ms in den Simulator einspeist. Die Fehllenkung fand vor der zweiten Pylonengruppe des Ausweichtests statt d.h. an der Stelle mit maximalem Lenkradausschlag (Abbildung 13).

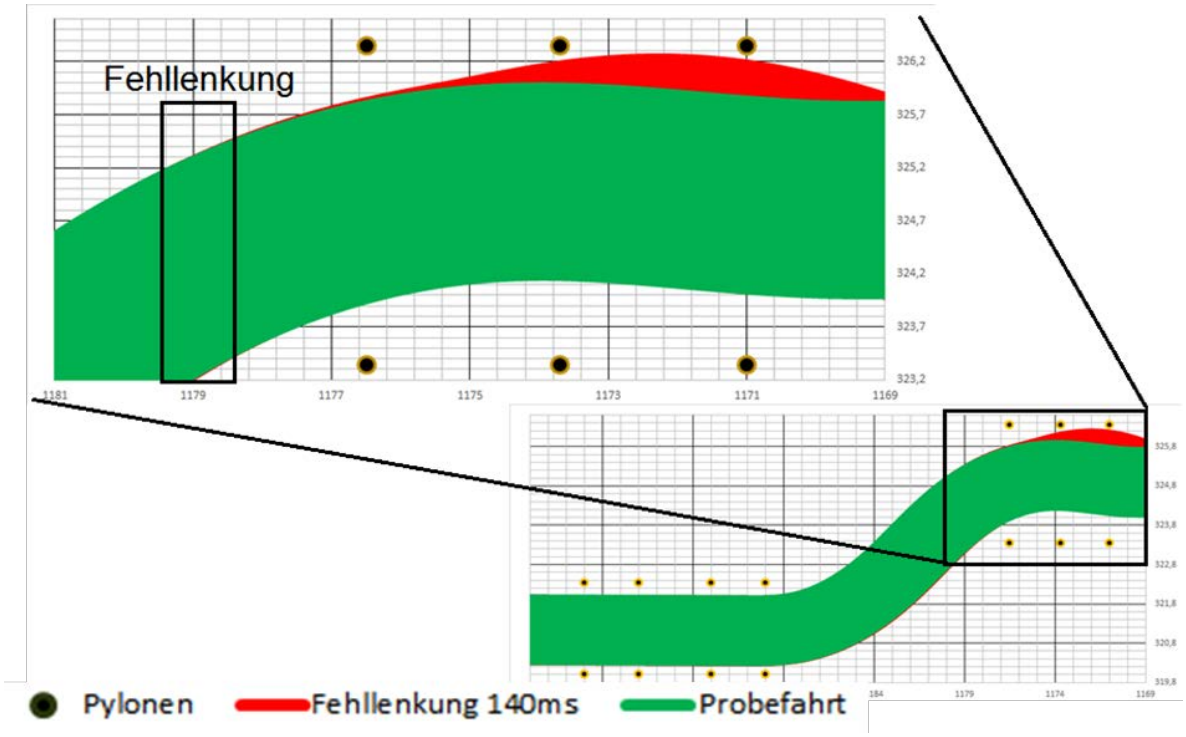

Abbildung 13: Darstellung des VDA-Ausweichtest mit Fehllenkungen für 140 ms bei ca.50 km/h

Während in Abbildung 13 die grüne Linie eine Referenzfahrt bei 50 km/h darstellt, bildet die rote Linie die Fahrt mit der Fehllenkung für 140ms ab. Die Pylonengasse ist mit Punkten dargestellt. Wegen einer Verzögerung durch die Fahrdynamik ist die Auswirkung der Fehllenkung erst später zu sehen. Dabei wurde das EPS für die Lenkung ausgeschaltet.
Aus den Fahrzeugtrajektorien folgt, dass bei einer Fehlenkung für 140ms das Fahrzeug noch den VDA-Ausweichtest schafft. Der gemessene Wert für die Abweichung von der Referenztrajektorie entspricht in etwa auch dem simulierten Wert.

Abgeschlossen wurde AP5 durch eine Validierungsphase, in der die Konfigurationen vorab in einer virtuellen Umgebung getestet wurde. Ein wesentlicher Punkt dabei waren die aus der Zeitanalyse des Reglers abgeleiteten zeitlichen Anforderungen (AP 1), die während dieser Tests verifiziert werden konnten.

Das eigentlich geplante **AP6** Entwicklung einer betriebssicheren Energieversorgung entfiel durch den Ausstieg von Leoni aus dem Projekt. Dies schränkte die Entwicklung der ausfallsicheren Aktorikansteuerung nicht ein, da sie unabhängig von der Betrachtung der Energieversorgung ist. Die verbliebenen Partner BMW, EMFT, Hella, Intedis und ITK führten das Projekt AutoKonf daher weiterhin wie geplant durch. Da die Validierung der ausfallsicheren Energieversorgung entfiel, rückte die Übernahme der verschiedenen Funktionalitäten stärker in den Fokus. Die Umsetzung des Versuchsaufbaus konnte durch die Lieferung der benötigten Kabelbäume von Leoni wie geplant umgesetzt werden.

Ebenfalls parallel zu AP4 und AP5 wurde vom Fraunhofer-IZM die Entwicklung der rekonfigurierbaren Steckverbindung angestoßen (**AP7**). Die Entwickler haben sich in diesem Arbeitspaket auf die Integration der Schaltfähigkeit in Steckverbinder und Schnittstellenmodule konzentriert. Sie erforschten dabei, welche klassischen Schaltmatrizen oder neuartige Verfahren auch auf kleinstem Bauraum zuverlässig funktionieren. Zudem wurde für die Aufbau- und Verbindungstechnik ein thermisches Design entwickelt.
Zunächst haben die Projektpartner entsprechend der Anforderungen aus den vorherigen Arbeitspaketen ein Schaltkonzept entworfen, das sich in die Teile Daten und Leistung gliedert. Im Vordergrund standen dabei das Schalten der Daten mit hoher Leitungsanzahl und in Hinblick auf die Leistung die hohe Stromdichte im begrenzten Bauraum. Zudem musste das Konzept Interferenzen zwischen Daten- und Energiefluss ausschließen.
Dazu wurde von den beteiligten Partnern evaluiert, ob klassische Schaltelemente wie Schalter oder Transistoren unter den gegebenen Rahmenbedingungen, z. B. Umweltbelastungen, Zuverlässigkeit, Reaktionszeit, EMV oder Kostenstruktur, für die Aufgabe in Frage kommen. Zusätzlich erarbeiteten die Entwickler alternative, speziell für die Anforderungen optimierte Konzepte. Dabei wurde eine Methodik eingesetzt, die nicht auf einfachem Re-Routing mit Transistoren beruht, sondern nur für den speziellen Fall eines Steuergeräteausfalls ausgelegt ist. Dabei wurden die Leistungsströme im Normalbetrieb nicht über Schaltelemente geleitet, da dies, im Gegensatz zu einer direkten Leitung, die Zuverlässigkeit der Übertragung reduziert (Abbildung 14). Das Konzept wurde abschließend als Funktionsdemonstrator validiert und in speziell ausgewählte Steckverbinder integriert. Der Demonstrator wurde auf die geforderte Fehlerfreiheit bewertet und daraus notwendige Mindestanforderungen für das untersuchte Teilnetz bezüglich „autonomes Fahren“ abgeleitet.

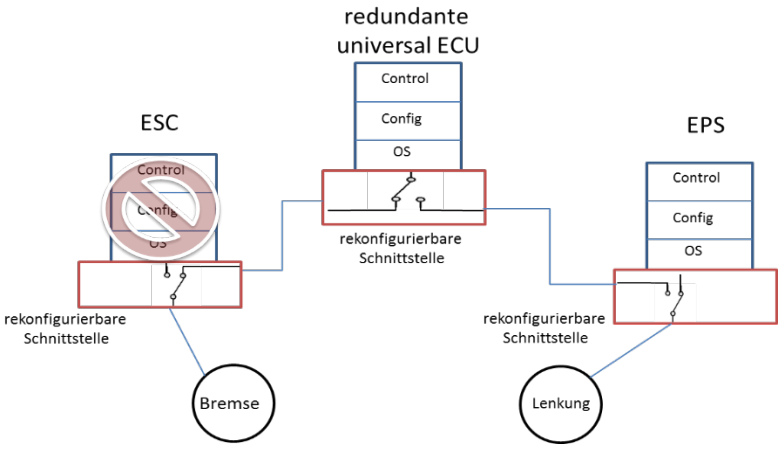

Abbildung 14: Grundfunktion der rekonfigurierbaren Schnittstelle

Mit dem Musteraufbau in **AP8** wurde bereits während der parallel laufenden Komponentenentwicklung begonnen. Sobald die für den Aufbau notwendigen Anforderungen an den Prüfstand aus den Arbeitspaketen fixiert waren (Zeitanalyse des Reglers (AP4), ECU-Konfiguration (AP5), AVT-Funktionsmuster (AP7)), konnte AP8 starten. Zudem bereiteten die Entwickler bereits in AP8 die Systemvalidierung im Vehicle Hardware-In-The-Loop (VeHil) vor, und planten die dafür notwendigen Szenarien final. Das verwendete Fahrzeugmodell musste dabei so angepasst werden, dass die Rekonfigurierbarkeit der Chassis-ECUs möglich wurde. Das Modell wurde für das Beispielfahrzeug kalibriert und mit einer Regelung für die Fahrdynamik versehen, um die Einflüsse der Rekonfiguration auf die Fahrzeugstabilität realistisch untersuchen zu können. Zur Versorgung des Fahrzeugmodells mit den benötigten Eingangssignalen wurden die festgelegten Fehlerszenarien aufgebaut und vorab getestet.
Für den Musteraufbau wurden die von den Partnern entwickelten Systemkomponenten in den Prüfstand integriert. Jeder Partner hatte dabei genug Zeit, die Funktionsmuster an den Prüfstand anzupassen. Vor allem die Funktionalität, das mechanische Design, die Robustheit der Komponente und die thermische Stabilität sollten von den Entwicklern sichergestellt werden, bevor der Prüfstand fertiggestellt war (Abbildungen 15 und 16).
Die Partner strebten beim Musteraufbau einen möglichst hohen Automatisierungsgrad an, damit bei Änderungen im System die definierten Szenarien bei der späteren Validierung ohne großen Aufwand wiederholt werden konnten. Finalisiert wurde AP8 durch einen detailliert ausgearbeiteten Validierungsplan, in dem die Partner die einzelnen Schritte zur Prüfung des automatisch rekonfigurierbaren Systems präzise festlegten.

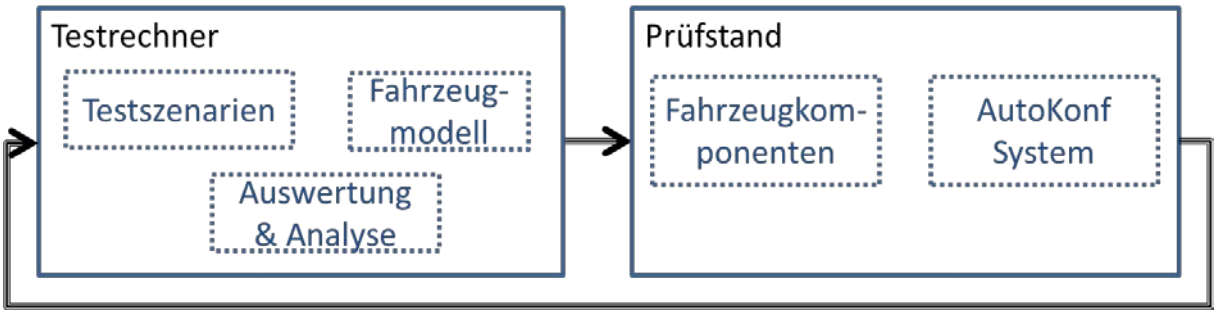

Abbildung 15: Struktureller Aufbau des Prüfstands in AP8

Abbildung 16: Musteraufbau mit den entwickelten Komponenten bei Intedis

Im abschließenden **AP9** wurde die Systemvalidierung im Vehicle Hardware-In-The-Loop (VeHIL) durchgeführt, wobei die Projektpartner den zuvor definierten Validierungsplan umsetzten. Dabei wurden die Testergebnisse dokumentiert, Abweichungen zu den Anforderungen herausgestellt, und die Gesamtergebnisse allen Beteiligten zur Verfügung gestellt. Mithilfe der Abweichungen konnte die Systemvalidierung auch genutzt werden, um in den iterativen Validierungsschleifen Verbesserungen am System oder Komponenten durch die Partner umzusetzen. Dadurch ergab sich eine Testschleife in der zyklisch Tests, Auswertungen und Optimierungen solange ausgeführt wurden, bis die Anforderungen an das System abgedeckt waren. Daneben wurden für spezielle Validierungen, wie sie etwa am Anfang der Validierung oder für wichtige Veröffentlichungen notwendig waren, von Intedis Workshops mit den beteiligten Partnern organisiert.

Nach durchlaufen der Testschleifen fertigten die Partner einen detaillierten Validierungsbericht an, der neben den abschließenden Ergebnissen der Systemtests auch eine Beschreibung des modifizierten Prüfstands enthält und aufzeigt, dass alle Anforderungen an die automatisch rekonfigurierbare Aktorikansteuerung vollständig erfüllt werden. Als der Nachweis der Tragfähigkeit des Systems erbracht war, erfolgte die abschließende Freigabe des Systems bzw. der einzelnen Komponenten durch alle Verbundpartner. Zudem wurde von allen Projektpartner gemeinsam ein Ergebnisdokument erstellt, in dem neben dem Nachweis der Tragfähigkeit des Konzepts auch für zukünftige Systeme dargelegt wurde.

2. Wichtigste Positionen des zahlenmäßigen Nachweises

Die gesamten Kosten von BMW sind im Zwischennachweis für Zuwendungen auf Kostenbasis (ZNZK) aufgeführt. Zu den wesentlichen Kostenfaktoren von BMW zählten vor allem Personalkosten für Mitarbeit von qualifizierten Entwicklungsingenieuren am Projekt. Eine weitere

wichtige Kostenposition ist der Unterauftrag an Silver Atena von BMW in Hinblick auf die Unterstützung bei der Entwicklung der Chassis-ECU und des Vernetzungskonzepts. Dies beinhaltete auch den Aufbau der Simulationsumgebung

3. Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die Entwicklungsarbeiten im Projekt AutoKonf behandelten aktuelle Fragestellungen in Hinblick auf redundante, fehlertolerante Steuerungssysteme für voll- und hochautomatisierte Fahrzeuge. Die dabei eingesetzte automatische Rekonfiguration von Steuergeräten stellt eine Innovation dar, da diese Methode bislang nicht im automobilen Umfeld zur Anwendung kam. Zudem wurde durch den neuen Ansatz aus dem Projekt gezeigt, dass durch die Möglichkeit der Rekonfiguration ein redundantes Steuergerät die Funktionalitäten zweier komplexer Aktorikansteuerungen darstellen kann und damit die Gesamtanzahl redundanter Steuergeräte reduziert werden kann.
Um die Projektziele zu erreichen, hat sich ein engagiertes und kompetentes Forschungskonsortium, bestehend aus Partnern der Großindustrie, des Mittelstandes und der Wissenschaft gebildet. Die Partner ergänzten sich in ihren Kompetenzen und Handlungsfeldern ideal. Durch die Zusammensetzung des Konsortiums konnten alle wichtigen Forschungsfragen und Entwicklungsschritte des Projekts selbstständig gelöst werden. Lediglich bei den Entwicklungen des Chassis-ECUs und des Vernetzungskonzepts nahmen die Projektpartner für den Aufbau, die Integration und die Validierung einer Simulationsumgebung externe Unterstützung in Form eines Unterauftrags in Anspruch. Alle anderen Forschungs- und Entwicklungsleistungen wurden von den Projektteilnehmern selbst erbracht.

Alle im Bericht dargestellten Arbeiten und Entwicklungen waren für das Erreichen der Projektziele notwendig. Die Aufwände für die Forschungs- und Entwicklungsarbeiten stehen dabei in Relation zur Komplexität und Relevanz der jeweiligen Aufgabe. Die technische und wissenschaftliche Bedeutung bzw. Relevanz der Projektergebnisse konnte durch Fachvorträge und Beiträge zu internationalen Symposien und Konferenzen unterstrichen und belegt werden. Zudem haben sich vielfältige Möglichkeiten für Anschlussprojekte ergeben, da das Projekt AutoKonf das erste Forschungsvorhaben im Bereich der automatische rekonfigurierbaren Aktorikansteuerungen für automatisierte Fahrzeuge war.

4. Erfolgte oder geplante Veröffentlichungen der Ergebnisse

Bereits während der Laufzeit, als auch nach Abschluss des Projekts sind bereits Veröffentlichungen von Projektergebnissen erfolgt. Auf branchenrelevanten Symposien und Konferenzen stellten die Teilnehmer die Ergebnisse einem internationalen Fachpublikum aus Industrie und Wissenschaft vor. Die ausgearbeiteten Vorträge wurden in Auszügen auch in den Veranstaltungsunterlagen veröffentlicht.
Folgende Veröffentlichungen sind im Rahmen des Teilprojekts bislang erfolgt:

- **Orlov, Sergey; Korte, Matthias; Oszwald, Florian; Vollmer, Pascal** (2020): *Automatically reconfigurable actuator control for reliable autonomous driving functions (AutoKonf).* In: Peter E. Pfeffer (Hg.): 10th International Munich Chassis Symposium

2019. Chassis.tech plus. München, 2019-06-25/2019-06-26. 1st ed. 2020: Springer Vieweg (Proceedings), S. 355–368.

- **Oszwald, Florian; Obergfell, Philipp; Traub, Matthias; Becker, Jürgen** (2019): *Reliable Fail-Operational Automotive E/E-Architectures by Dynamic Redundancy and Reconfiguration.* In: Proceedings of the 32nd IEEE International System-on-Chip Conference (SOCC). Singapur, 2019-09-03/2019-09-06.

- **Oszwald, Florian; Obergfell, Philipp; Traub, Matthias; Becker**, Juergen (2018): *Using Simulation Techniques within the Design of a Reconfigurable Architecture for Fail-Operational Real-Time Automotive Embedded Systems.* In: IEEE International Symposium on Systems Engineering (Hg.): 2018 IEEE International Symposium on Systems Engineering. 2018 IEEE International Symposium on Systems Engineering. Rome, 2018-10-01/2018-10-03, S. 1–3.

- **Oszwald, Florian; Becker, Jürgen; Obergfell, Philipp; Traub, Matthias** (2018): *Dynamic Reconfiguration for Real-Time Automotive Embedded Systems in Fail-Operational Context*. In: 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). Vancouver, BC, Canada, Canada, 2018-05-21/2018-05-25, S. 206–209.

Weiterhin bleibt auch die Internetseite **www.autokonf.de** frei verfügbar. Sie bietet durch Videos, Bilder und Texten allen Interessierten frei verfügbare Informationen, die natürlich auch den Projektpartnern für weitere Veröffentlichungen oder Arbeiten zur Verfügung steht.

Literaturverzeichnis

[1] finanzen.net. finanzen.net. [Online] 7.1.2016; http://www.finanzen.net/nachricht/aktien/UPDATE-Was-die-Autoindustrie-auf-der-CES-zum-Thema-autonomes-Fahren-sagt-4677631.

[2] Vetter, Philipp. Die Welt. [Online] 14.9.2015; http://www.welt.de/wirtschaft/article146385922/Google-baut-das-Auto-und-Daimler-liefert-zu.html.

[3] Bundesregierung. *Strategie automatisiertes und vernetztes Fahren.* Berlin : Bundesregierung, 2015.

[4] Bundesministeriums für Wirtschaft und Energie. Hochautomatisiertes Fahren Auf Autobahnen. Berlin : s.n., 2015.

[5] Merat, Natasha. Transition to manual: Driver behaiviour when resuming control from a highly automated vehicle. s.l. : Elsevier Verlag, 2014.

[6] Damböck, Daniel. Automationseffekte im Fahrzeug – von der Reaktion zur Übernahme. München : s.n., 2013.

[7] Gold, Christian, et al., et al. "Take over!" How long does it take to get the driver back into the loop? 2013.

[8] Grabs, Peter. E/E architecture proposals for automated driving and their failure robustness. Bad Boll : EEHE, 2015.

[9] Kaewkerd, Watana. Steer-By-Braking. Würzburg : Intedis , 2014.

[10] Armbruster, S. Synergies in the development of powernets for X-by-wire-Systems and Aircraft Concepts – Realisation in the European Project SPARC. Hannover : Forum Electrical Energy Distribution Systems, 2005.
[11] Prechler, Reinhard. Trends und Herausforderungen im Bordnetz. Ingolstadt : s.n., 2014.
[12] Karimi, H. A. Big Data: Techniques and Technologies. Geoinformatics : CRC Press, 2014.
[13] Jurgen, R. K. X-By-Wire Automotive Systems. s.l.: SAE International, 2009.
[14] Bryan Peter Riddiford, Ernst Severin Baumgartner. Brake by wire system with BTSI based vehicle operation control. US6709069 B2 USA, März 23, 2004.
[15] William Spadafora, David Llewellyn, Perry Paielli, Jason Kramer. Failure mode effects mitigation in drive-by-wire systems. US8234045 B2 USA, Juli 31, 2012.
[16] Kevin P. Roy, Thaddeus J. Zebrowski. Electronic engine control software reconfiguration for distributed eec operation. US20120095662 A1 USA, April 19, 2012.
[17] Valentina Salapura, Robert W. Wisniewski. Hardware support for software controlled fast reconfiguration of performance counters. US8543738 B2 USA, September 24, 2013.

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung

3. Titel
Reliable Fail-Operational Automotive E/E-Architectures by Dynamic Redundancy and Reconfiguration

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens
Oszwald, Florian; Obergfell, Philipp; Traub, Matthias; Becker, Jürgen	6. Veröffentlichungsdatum 2019-09-03/2019-09-06
	7. Form der Publikation Paper

8. Durchführende Institution(en) (Name, Adresse)	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 16EMO0205
	11. Seitenzahl 6

12. Fördernde Institution (Name, Adresse)	13. Literaturangaben
Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	14. Tabellen
	15. Abbildungen

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)

18. Kurzfassung

For future autonomous driving cars, fail-operational systems are necessary. Dynamical reconfiguration is one possible approach to fulfill this requirement for fail-operational behavior. For automotive real-time embedded systems in a failoperational context, dynamical reconfiguration has not yet been investigated. At first, this paper describes a process to realize this approach in the automotive industry and shows its advantages.
Second, we adopt an existing fail-operational architecture to the requirements of the steering function and extend the existing state handover with the CAN communication. For this, we modeled a hardware extension to prevent the system from a loss of state and integrated it into this architecture. Third, we integrate the adapted architecture into a service-oriented architecture, and specify necessary interfaces and protocols. By using a service-oriented approach, we enhance the principle of dynamic redundancy from the component level to the system level. As an evaluation, we provide an implementation on a test bench which reveals indications for the use of our concept in future autonomous driving cars.

19. Schlagwörter
Real-time embedded systems, fail-operational, automotive, dynamical reconfiguration, simulation

20. Verlag	21. Preis

Document Control Sheet

1. ISBN or ISSN 10.1109/SysEng.2018.8544451	2. type of document (e.g. report, publication)
3. title Using Simulation Techniques within the Design of a Reconfigurable Architecture for Fail-Operational Real-Time Automotive Embedded Systems	
4. author(s) (family name, first name(s)) Oszwald, Florian; Obergfell, Philipp; Traub, Matthias; Becker, Juergen	5. end of project 31.10.2019
	6. publication date 2018-10-01/2018-10-03
	7. form of publication
8. performing organization(s) (name, address) BMW AG München	9. originator's report no.
	10. reference no.
	11. no. of pages
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references
	14. no. of tables
	15. no. of figures
16. supplementary notes	
17. presented at (title, place, date)	
18. abstract In the automotive industry one clear goal is to reach the fourth SAE level of driving automation. Instead of having a redundant E/E-architecture we propose a dynamically reconfigurable one. With this paper we introduce two new simulation techniques on how to extract two important values for reconfiguration. The approach is based on an example for the loss of steering control functionality. The first value is the overall system reconfiguration time that is recognized by the human driver in case of a loss of steering control functionality. The second value is the maximum reconfiguration time possible to still perform a given maneuver. The results of both values are compared to a previous study. This leads to end-to-end reconfiguration times for future development of fail-operational self-reconfigurable realtime automotive embedded systems. A method for simulating loss of functionality and deriving specification relevant data is given to assist the automotive industry reaching fail-operational systems. It will also help in introducing dynamical reconfiguration for a fail-operational automotive E/E-architecture as the next step.	
19. keywords	
20. publisher	21. price