Bundesministerium
für Bildung
und Forschung

Schlussbericht zum Vorhaben

Nanoelectronics for Electric Vehicle Intelligent Failsafe PowerTrain

(Kurztitel MotorBrain)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16N11480 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Zuwendungsempfänger	OFFIS	**Förderkennzeichen**	16N11480
Vorhabensbezeichnung	MotorBrain		
Laufzeit des Vorhabens	01.07.2011-30.06.2014		
Berichtszeitraum	01.07.2011-30.06.2014		
Autoren	Dr.-Ing. Sven Rosinger, Kim Grüttner, Maher Fakih		

Inhaltsverzeichnis

I. Kurze Darstellung

Das primäres Ziel von MotorBrain war die Entwicklung eines intrinsisch ausfallsicheren, fehlertoleranten und hoch-effizienten Antriebsstrangs für Elektrofahrzeuge, basierend auf neuen Elektromotoren, neuartiger Leistungselektronik, innovativem Packaging für die Leistungselektronik sowie leistungsfähigen und sicheren Kontrollansätzen für den integrierten Antriebsstrang.

Das Gesamtziel von MotorBrain sollte zu einem signifikanten Fortschritten und einer 20% Effizienzsteigerung des Gesamtsystems führen, durch

1. Die Entwicklung von leichteren hoch-effizienten , hoch-integrierten und zuverlässigen elektrischen Antrieben
2. Neuartige Elektromotoren mit Integration der Leistungselektronik in den Motor unter Einsatz innovativer industrieller Fertigungsprozesse für die Herstellung von leichten, kostengünstigen Motoren unter Nutzung neuer Materialien zur Beseitigung der potentiellen Abhängigkeit von China im Hinblick auf Rohstoffe für heute eingesetzte Permanentmagnete.
3. Nutzung bidirektionaler 10 kW Wandler mit Steuerelektronik zum Laden und Entladen der Batterien
4. Nutzung innovativen Antriebsstrangarchitekturen mit integriertem Sicherheitskonzept unter Nutzung leistungsfähiger, skalierbare Multicore-Controller.

Die Arbeiten von OFFIS am MotorBrain Projekt waren vor allem durch die hohen Sicherheitsanforderungen (ASIL D = höchste Sicherheitsstufe) die an einen vollelektrischen Antriebsstrang gestellt werden motiviert. Diese Anforderungen konnten zum Start des Projekts von der Automobilindustrie insbesondere bei der Nutzung Multicore-Controllern noch nicht kosteneffizient erfüllt werden.

Das Ziel von OFFIS war es Methoden und Techniken für einen durchgängigen Entwicklungsprozess der elektronischen Steuerung eines vollelektrischen Antriebsstrangs zu erforschen. Dieser Entwicklungsprozess sollte modellbasiert (d.h. es sollten ausführbare Modell auf unterschiedlichen Abstraktionsebenen erstellt werden, die zunächst in einer simulierten Umwelt getestet und nach der Implementierung im Zielsystem mit den Modellen verglichen werden sollten) und kompatibel zu dem Sicherheitsstandard ISO CD 26262 („Road vehicles – Functional safety“) sein.

Die Aufgaben von OFFIS ordnen sich damit in die oben beschriebenen Unterziele 1 und 4 ein.

I.1 Aufgabenstellung

Der von OFFIS erforschte Entwicklungsprozess wurde in das MotorBrain Projekt entlang der Arbeitspakete 1, 2, 3 und 6 durchgeführt und enthielt die folgenden Aufgaben:

- Erfassung und Formalisierung von Anforderungen, um sie im modellbasierten Entwurf in allen Verfeinerungsstufen zu berücksichtigen
- Sicherheitsanalyse der funktionalen und physikalischen Architektur begleitend zum Entwurfsprozess (vgl. ISO CD 26262)
- Modellbasierte Entwurfsmethodik, mit folgenden Eigenschaften:
  - Inkrementeller Entwurfsablauf, der unterschiedliche, klar definierte Abstraktionsebenen und eine Verfeinerung ermöglicht.
  - Möglichkeit formale funktionale und nicht-funktionale Anforderungen auszudrücken
  - Nachverfolgbarkeit der Anforderungen über die unterschiedlichen Abstraktionsebenen hinweg
- Methoden und Techniken zur Spezifikation, Implementierung und Analyse von Hardware- & Software-Komponenten des „Control Layers“ eines vollelektrischen Antriebsstrangs (bestehend aus Dual-Core Prozessoren und gemeinsam genutzten Ressourcen)
- Verifikation und Validierung der implementierten Kontrollalgorithmen im Zusammenspiel mit der eingesetzten Hardware (ECUs, Kommunikationsbusse, Transceiver, etc.)

- Echtzeitanalyse im funktionalen Modell der Kontrollsoftware entsprechend den ermittelten Anforderungen
- Simulation & Test der Kontrollsoftware nach der Implementierung auf der Hardware.

Diese Aufgabenstellung integriert sich in die Gesamtaufgabenstellung, die im ausführlichen Verbundschlussbericht des Projektes beschrieben wird.

I.2 Voraussetzungen unter denen das Vorhaben durchgeführt wurde

Die in MotorBrain adressierten Themen sind von hoher industrieller Relevanz, aber auch die zugrundeliegenden wissenschaftlichen Themen stellen eine Herausforderung zur Lösung der Probleme dar. Hier kann OFFIS auf einschlägige Vorarbeiten in nationalen und europäischen Projekten (teilweise auch als industrieller Unterauftragnehmer) zurückgreifen (u.a. SPEEDS, COMBEST, CESAR, SPES2020, SPEAK, SPEAK 2, VISION, SANITAS), die im Kontext von MotorBrain genutzt, erweitert und optimiert werden konnten.

ArtistDesign – Design of Embedded Systems ist ein Exzellenznetzwerk im 7. Rahmenprogramm der EU und bündelt das Know-how von etwa 30 europäischen Universitäten und Forschungsinstituten zum Entwurf eingebetteter Systeme und gliedert sich in mehrere thematische Cluster: „Modeling and Validation“; „SW Synthesis“, „Code Generation and Timing Analysis“; „Operating Systems and Networks“; „Hardware Platform and MPSoCs“, sowie in clusterübergreifende Aktivitäten, die insbesondere Anwendungsaspekte im industriellen Kontext untersuchen. OFFIS ist hier insbesondere im erstgenannten Cluster involviert. Durch den wissenschaftlichen Austausch auf der Ebene des Exzellenznetzwerkes ergeben sich Synergien, die in die Arbeiten von MotorBrain einfließen können.

Das unter Federführung von OFFIS gebildete Kompetenznetzwerk SafeTRANS (www.safetrans- de.org) bündelt die Forschungskompetenz des OFFIS FuE Bereichs Verkehr, des Forschungszentrums Sicherheitskritische Systeme der Carl von Ossietzky Universität Oldenburg, sowie der DLR Institute für Transportwesen und Flugsystemtechnik in Braunschweig, um in Kooperation mit führenden Unternehmen der Verkehrsbranche (unter anderem Airbus, Bosch, BTC Embedded Systems, Daimler, DLR, EADS, Siemens, ...) Methoden und Prozesse zur Entwicklung sicherheitskritischer eingebetteter Systeme im Rahmen einer gemeinsamen Forschungsstrategie zu entwickeln. SafeTRANS ist vom Land Niedersachsen als „International Center for Modelling and Analysis of Safe Transportation System“ ausgezeichnet worden.

I.3 Planung und Ablauf des Vorhabens

Das Projekt MotorBrain wurde für eine Laufzeit von drei Jahren geplant und startete im Juli 2011. MotorBrain gliederte sich in 8 Arbeitspakete, die jeweils von einem Projektpartner geleitet wurden. Die Arbeiten in den Supply Chains (SC) 2 und 8 erfolgten in Kombination, da SC8 als zu entwickelnde Controller-Plattform Teil des SC2-Demonstrators ist. Arbeiten bzgl. funktionaler Sicherheit und modell-basierter Software-Entwicklung decken dabei beide Supply Chains ab.

Die Arbeiten in den Supply Chains SC2 und SC8 erfolgten orthogonal zu den Arbeiten in den Arbeitspaketen. Dabei deckt WP1 die Arbeiten im Bereich der Spezifikation und Initiierung des Safety-Lifecycle ab. In WP2 wird das Sicherheitskonzept des SC2-Antriebsstrangs und der SC8-Controller-Plattform konkretisiert und validiert.

OFFIS ist Leiter des WP2 und koordiniert in der Funktion auch die Arbeiten der anderen Supply Chains (SC1, SC3, SC5, SC7) im Bereich des Sicherheitskonzepts. Diesen Supply Chains steht es frei, eigene Konzepte zur Umsetzung des ISO26262-Prozesses zur verwenden.

Die von OFFIS geplanten und erbrachten Beiträge verteilen sich wie folgt:

Arbeitspaket 1: “System level specification: Domains, Requirements, Partitioning”

OFFIS hat sich in diesem Arbeitspaket um die Formalisierung von Sicherheitseigenschaften und die Modellierung und Partitionierung von Funktionen gekümmert. Der Schwerpunkt lag hierbei auf dem Control Layer (Dual-Core CPU) inklusive des Bussystems und der Kommunikation mit anderen ECUs.

Wir unterstützen diese Arbeiten in den sogenannten „Application Areas“ mit den Titeln „Integrated EV Powertrain Concepts and Novel Engines“ und „EV powertrain control platform“. Dabei wurden die Industriepartner im Wesentlichen bei der Formalisierung ihrer Anforderungen unterstützt. Spezifikationen, die von Industriepartnern in strukturierter Sprache (z.B. structured english) vorgelegt wurden, konnten teilweile formalisiert werden, um sie im modellbasierten Entwurfsprozess rechnergestützt überprüfen und nachverfolgen zu können. Parallel dazu wurde ein funktionales Systemmodell der Antriebsstränge aus Supply-Chain 2 & 3 erstellt, welche die Eingabe für die weitere Verfeinerung in Arbeitspaket 2 und 3 darstellte. Das in diesem Arbeitspaket entstehende Systemmodell wurde zusammen mit den formalisierten Anforderungen in Form von sogenannten Kontrakten (engl. Contracts) repräsentiert. Mit Hilfe dieser formalisierten Anforderungen konnte in den nachfolgenden Arbeitspaketen eine Analyse bzgl. funktionaler, Zeit- und Sicherheitseigenschaften durchgeführt werden.

Arbeitspaket 2: “Safety and redundancy concepts implementation”

Der Hauptbeitrag von OFFIS in diesem Arbeitspaket war der Einsatz von Methoden zur Beurteilung von Allokationsentscheidungen von funktionalen Komponenten auf einem on-chip ECU-Netzwerk eines Multicore Controllers. Hierbei wurde sowohl die Allokation selbst, als auch die Topologie des ECU Netzwerks bezüglich dessen Auswirkungen auf Zeiteigenschaften und die damit verbundene funktionale Sicherheit betrachtet. Dies wurde durch die Erforschung und Bereitstellung eines für die industriellen Anwendungsfälle (in Supply-Chain 2 & 3) geeigneten Fehlerpropagationsmodells, welches die Komposition von qualifizierten und unqualifizierten Fehlern erlaubt, ermöglicht. Mit Hilfe der aus Arbeitspaket 1 in Form von Contracts formalisierten Anforderungen wurde somit eine Beschreibung möglicher Fehlerfälle ermöglicht. Das funktionale Modell mit Contracts, die möglichen Allokationsentscheidungen inkl. der Abbildung von Funktionen auf Architekturkomponenten und das Fehlerpropagationsmodell ermöglicht zusammen mit auszuwählenden Analysemethoden eine Überprüfung der Sicherheitsziele. Darüber hinaus ermöglicht die bereitgestellte Methode den Vergleich unterschiedlicher Architekturen bezüglich ihrer Sicherheitseigenschaften.

OFFIS hat dieses Arbeitspaket organisatorisch geleitet.

Arbeitspaket 3: "Brain- Safety critical control architectures”

Die in Arbeitspaket 2 bezüglich ihrer Sicherheitseigenschaften bewertete Allokation und Abbildung von funktionalen Einheiten auf ein on-chip ECU Netzwerk eines Multicore-Controllers wurde hier begleitend zur Implementierung bzgl. der Einhaltung der in Arbeitspaket 1 formalisierten Zeitanforderungen untersucht und bewertet. Hierzu wurde das rein funktionale Modell des vollelektrischen Antriebsstrangs aus Arbeitspaket 1 mit Hilfe einer modellbasierten Entwicklungsmethodik vom Deployment bis zur Implementierung auf den ECUs verfeinert. Zur Verifikation und Validierung der funktionalen und nicht-funktionalen Anforderungen während dieser Verfeinerungsstufen wurde ein hybrides Modell bestehend aus einer formalen Analyse und einer Simulation erforscht. Hierzu wurde aus dem funktionalen Modell ein Funktionsnetzwerk (erweitertes Task-Netzwerk) abgeleitet. Zusammen mit Ausführungszeiten der Tasks auf den zugewiesenen ECUs wurde eine statische Zeitanalyse (z.B. Schedulinganalyse, Überprüfung von End-to-End-Deadlines, …) durchgeführt. Die Ausführungszeiten pro Task wurden durch eine zyklusgenaue Simulation in einem ausführbaren Modell der ECUs und der Kommunikationsinfrastruktur ermittelt, weil für den verwendeten Prozessor noch kein WCET Analysewerkzeug zur Verfügung stand. Zur Überprüfung der Zeitanforderungen wurde dann die formale Analyse basierend auf Realzeitautomaten (inkl. der damit verbundenen Überapproximation) in Kombination mit einer zyklusgenauen Simulation der ECU-Plattform benutzt. In Absprache mit den Industriepartnern wurden nur statische Ablaufplanungen ohne Verwendung einer Realzeitbetriebssystems verwendet.

Arbeitspaket 6: EV integration and demonstrations

In diesem Arbeitspaket beteiligte sich OFFIS an der Integration der zentralen Antriebssteuerung in ein virtuelles Gesamtsystem bestehend aus einem Elektromotormodell und der Multi-Core ECU inklusive

dem Kommunikationsnetzwerk. Ziel der Arbeiten war es die Implementierung auf dem Multi-Core ECU-Prototyp für ausgewählte realisierte Funktionen gegen das analytische Modell und die Vorhersagen aus Arbeitspaket 3 zu vergleichen. Hierzu wurde von Infineon sowohl eine virtuelle Plattform als auch ein Evaluationsboard des AURIX Multi-Core Prototyps bereitgestellt. Der Vergleich mit den ausführbaren Modellen erfolgte dann für ein ausgewähltes Teilsystem der Motorsteuerung mit Hilfe einer Restbussimulation. D.h. die zu messende/testende Teilfunktion läuft auf dem ECU-Prototypen, während das Restsystem auf einem Hostrechner durch das funktionale System aus Arbeitspaket 3 simuliert wird. Dieser Ansatz wurde von einem einfachen Hardware-in-the-Loop (HIL) Ansatz für die einzelnen Steuerungsalgorithmen bis hin zu einer Integration in einen virtuellen Motorteststand (basierend auf einem Fahrsimulator mit Fahrdynamikmodell) zur Kopplung von ECU, Kontrollsoftware und Motorprototyp mit integrierten intelligenten Sensoren ausgebaut. OFFIS hat sich hierbei hauptsächlich auf einfachen HIL Ansatz konzentriert, um damit die in Arbeitspaket 3 erforschte Methodik bewerten zu können.

Arbeitspaket 7: Standardisation, Dissemination and Exploitation

Die im Rahmen der OFFIS-Beteiligung in den Arbeitspaketen 1 und 2 durchgeführten Arbeiten wurden stets kompatibel mit den Richtlinien der ISO 26262 durchgeführt. Ziel von OFFIS war es die Contract-basierte Entwurfsmethodik zur Unterstützung bei der Zertifizierung nach ISO 26262 weiter zu etablieren. Dies erfolgte vor allem durch die entsprechende Prozessunterstützung von Industriepartnern bei der Anwendung von ISO 26262 während der Spezifikationsphase und der Erarbeitung des funktionalen Sicherheitskonzepts.

Geplant war es, dass OFFIS die im Rahmen von MotorBrain entstehenden Erkenntnisse und Ergebnisse aus Arbeitspaket 3 und 6 in die entsprechenden AUTORSAR Arbeitsgruppen einbringt. OFFIS war auch über die Zeit in MotorBrain hinweg aktives AUTORSAR Development Mitglied ist und hat die Entwicklungen von AUTOSAR zur Unterstützung von Multicore-Controllern weiter mitverfolgt und dessen Einsatzmöglichkeiten im Projekt geprüft. Da sich im Projektverlauf jedoch herausgestellt hat, dass AUTOSAR für die Verwendung im Antriebsstrang (insb. unter Verwendung eines Multicore-Controllers) nicht gut geeignet ist, wurde von diesem Ziel wieder Abstand genommen. Die Erfahrungen und „Best Practices“ der in Arbeitspaket 2 entwickelten formalen Analysemethoden (siehe Abschnitt II), konnten allerdings in laufende Standardisierungsaktivitäten in den entsprechenden AUTOSAR Arbeitsgruppen eingebracht werden.

Als Forschungsinstitut haben wir Mitarbeitern die Möglichkeit zur Veröffentlichung der MotorBrain Projektergebnisse in internationalen Journalen und auf nationalen und internationalen Konferenzen, Seminaren und Workshops ermöglicht. Damit wurden auch explizit Promotionen zu den Forschungsarbeiten in MotorBrain unterstützt.

Die in MotorBrain erforschten Methoden und Ergebnisse, sowie das neugewonnene Wissen wurde in den an der Universität Oldenburg von OFFIS angebotenen Lehrveranstaltungen an die nächste Generation von Ingenieuren & Informatikern weitergegeben. Dies erfolgte in MotorBrain hauptsächlich durch die Ausschreibung themenrelevanter Master- und Bachelorarbeiten.

I.4 Wissenschaftlicher und technischer Stand an den angeknüpft wurde

Vor Beginn dieses Vorhabens wurden u.a. durch die Projekte SPEEDS, COMBEST, CESAR und SPES2020 bereits Methoden und prototypische Werkzeuge zur modellbasierten Anforderungsanalyse und Realzeitanalyse sicherheitsrelevanter Systeme erforscht und implementiert. Außerdem besaß OFFIS vor dem Projekt bereits umfangreiches Wissen zur ISO26262 und dessen Anwendung. Hier konnte das Wissen erfolgreich, am Beispiel des elektrischen Antriebsstrangs, angewendet und mit den industriellen Partnern geteilt werden.

Bzgl. der Zustandsbasierten Realzeitanalyse für Multi-Core Prozessoren mit gemeinsam genutzten Bussen, wurde im Rahmen dieser Arbeit ein neuen Verfahren erforscht, bei dem erstmalig die

Kombination aus Synchonous Data Flow Timing-Analyse auf einer MPSoC Architektur mit Hilfe von Realzeitautomaten durchgeführt wurde. Dies ist mit zahlreichen aus dem Projekt hervorgegangen Veröffentlichungen, auf hochrangingen internationalen Konferenzen und Journalen, belegt.

Bzgl. der virtuellen Integration und Fehlerinjektion/Fehlereffektsimulation, konnte auf Vorarbeiten aus den Forschungsprojekten SPEAK, SPEAK 2, VISION und SANITAS zurückgegriffen werden. Die bestehenden Techniken wurden durch die Emulation des Modells eines mehrphasigen Elektromotors auf einem Raspberry Pi erweitert. Diese Lösung wurde in dieser Form erstmalig in der Fachliteratur vorgeschlagen und ergänzt das Spektrum teurer Hardwarespeziallösungen für die Emulation mit einer kostengünstigen und leicht erweiterbaren Infrastruktur.

I.5 Zusammenarbeit mit anderen Stellen

Das Projekt wurde von Rainer John (Infineon) mit administrativer Unterstützung von Alfred Höß (HF Johanneum) koordiniert. Das Projektmanagementteam (PMT) setzte sich aus dem Koordinator, seinem Vertreter und den Arbeitspaketleitern zusammen.

Zur Leitung des Projekts wurden regelmäßige Meetings und Partnerversammlungen veranstaltet sowie regelmäßige Telefonkonferenzen durchgeführt. Die in Kapitel I.3 beschriebene Unterteilung des Projekts in Arbeitspakete hat ebenfalls die Beiträge durch einzelne Partner festgelegt. Als wichtiges Arbeitspaket übergreifendes Instrument wurden Meilensteine definiert, um die Zusammenarbeit im Projekt zu stärken. Besonders hervorzuheben ist sind die orthogonal zu den Arbeitspaketen liegenden Supply Chains (SC). Diese waren ein effektives Instrument zur Bündelung von Aktivitäten in den unterschiedlichen Subdomänen des Projektes. Die wesentlich Kooperation (abgesehen von der Kooperation mit allen AP2 Partner, aufgrund unserer Leitungsfunktion) von OFFIS mit anderen Projektpartner fand im Rahmen von SC2 und SC8 statt. Hier ist, wie weiter unten beschreiben vor allem die Zusammenarbeit mit Infineon, ZF und AVL zu erwähnen.

II. Eingehende Darstellung

II.1 Erzielte Ergebnisse

Die im Projekt erzielten Ergebnisse werden im Folgenden nach Arbeitspakten aufgeschlüsselt dargestellt.

Arbeitspaket 1: System level specification: Domains, Requirements, Partitioning

Wir haben uns auf die Mitarbeit an der Spezifikation und Anforderungsdefinition des elektrischen Antriebsstrangs der **Supply Chain 2** (SC2) mit dem Fokus auf sicherheitsrelevanten Eigenschaften und Anforderungen auf Fahrzeugebene beschränkt. Wichtige erzielte Ergebnisse sind hier:

- Entwicklung und Vorstellung des in SC2 benutzten, auf dem V-Modell basierenden, Entwicklungsmetamodells (Common Meta Model, CMM) für die vollständige Erfassung und Darstellung aller Entwicklungsschritte von der initialen funktionalen Spezifikation bis zur Implementierung. Im Gegensatz zu bisherigen Ansätzen deckt das Modell gleichzeitig verschiedene Abstraktionsebenen (z.B. System-Ebene, Geräte-Ebene, Einheiten-Ebene, …) und Perspektiven (z.B. Funktionale Perspektive, Geometrische Perspektive, Technische Perspektive) ab.
- Erstellung und Kommunikation des Konzepts eines standardisierten Prozessmodells für die Durchführung der von der ISO26262 geforderten Entwicklungsschritte für funktionale Sicherheit (Item Definition → Hazard Analysis and Risk Assessment → Safety Concept → Safety Validation). Die Durchführung und Anwendung dieses Konzepts ist Teil von Arbeitspaket 2 (siehe unten).
- Diese Arbeiten erfolgen in enger Zusammenarbeit mit den SC2 Partnern Infineon (Deutschland), ZF (Deutschland), AVL (Österreich) und ermöglichten die Initiierung des Safety-Lifecycles.

Neben SC2 hat sich OFFIS um den konzeptionellen Entwurf eines Entwicklungsprozesses für die modell-basierte Softwareentwicklung auf Basis der in **Supply Chain 8** (SC8) entwickelten ECU-Plattform mit folgenden Eigenschaften gekümmert:

- Besondere Spezialisierung auf Automotive-Entwicklungen unter Beachtung von ISO26262
- Fokus auf sicherheitsrelevante Funktionen der Aurix/TriCore-Plattform
- Einbeziehung und Verknüpfung verschiedener Modelle (funktionale Modelle, Architekturmodelle, Simulationsmodelle)
- Kombination analytischer und simulations-basierter Test- und Verifikationsverfahren zur effizienten funktionalen Verifikation von Multi-Core-Systemen
- Verknüpfung von Anforderungen mit Komponentenmodellen
- Anforderungsgetriebene Analysen (z.B. Konsistenzprüfung, Nachverfolgbarkeit)
- Entwicklung eines Konzepts zur virtuellen Modellierung und Simulation der SC8 ECU-Plattform für frühzeitige funktionalen Verifikation von Controller-Software und Sicherheitsfunktionen sowie frühzeitige Integrationstests (Virtual Hardware-In-The-Loop)

Arbeitspaket 2: "Safety and redundancy concepts implementation"

Es wurde ein standardisiertes Prozessmodell für die Durchführung der von der ISO26262 geforderten Entwicklungsschritte für funktionale Sicherheit zur Anwendung in den Supply Chains SC2 und SC8 entwickelt und zusammen mit den Industriepartnern Infineon, ZF und AVL implementiert.

OFFIS hat in Kooperation mit anderen SC2/8-Partnern (insbesondere Infineon, ZF und AVL) zur Realisierung der entsprechenden Prozessschritte bis einschließlich des „Functional Safety Concepts" im Rahmen des MotorBrain-Demonstrators beigetragen.

Im Folgenden werden die einzelnen Schritte und Ergebnisse des entwickelten Prozessmodells für SC2 und SC8 näher erläutert:

- Initial wurde eine „Item Definition" durchgeführt und in Deliverable D1.14 dokumentiert. Dabei wurde die zu entwickelnde Komponente (in diesem Fall ein elektrischer Antriebsstrang) auf Systemebene einschließlich ihrer Einsatzumgebung (Fahrzeug der Kompaktklasse) und Anforderungen spezifiziert. Die Item Definition stellt den Ausgangspunkt für die weitere Entwicklung der Komponente und den Safety-Lifecycle dar.
- Darauf aufbauend wurde ein "Hazard Analysis and Risk Assessment" durchgeführt. Die Ergebnisse sind ebenfalls in Deliverable D1.14 dokumentiert sowie in einem in Abbildung 1 dargestellt. Innerhalb der HARA werden sogenannte *Hazards* (Gefahren, Risiken) des *Items* systematisch klassifiziert und auf ihr Gefahrenpotential hin analysiert.
- Ausgehend von identifizierten ungewollten *Hazards* sowie einer zugehörigen Risikobewertung wurden *Safety Goals* abgeleitet. Jedem Safety Goal ist ein entsprechendes *Automotive Safety Integrity Level* (ASIL) zugeordnet aus dem sich Anforderungen bzgl. der Implementierung der entsprechenden Systemfunktionen und Subkomponenten ergeben. Für den SC2 Antriebsstrang haben sich Safety Goals im Bereich QM (niedrigste Stufe, abgedeckt durch Standard-Qualitätsmanagement) bis hin zu ASIL C (zweithöchste Stufe, sehr hohe Anforderungen) ergeben.
- Aufbauend auf den allgemeinen Safety Goals wurden im weiteren Verlauf das *Functional Safety Concept* entwickelt (Auszug in Abbildung 3). In dem Rahmen wurden die Safety Goals in mehrere *Safety Requirements* verfeinert und den einzelnen Komponenten zugeordnet. Aus den mit den Safety Goals verbundenen Risiken ergaben sich erste konkrete Anforderung bzgl. der Umsetzung von einzelnen Funktionen und entsprechenden Gegenmaßnahmen zur Fehlervermeidung oder -kompensation.
- Im Rahmen der Fortsetzung des ISO26262 Safety Lifecycle wird das Functional Safety Concept im Projektjahr 2013 zum „Technical Safety Concept" weiterentwickelt und von OFFIS methodisch auf die Abdeckung der ursprünglichen Safety Goals hin verifiziert werden. Die entsprechenden Ergebnisse sind in den Deliverables D2.3, D2.8 und D2.9 dokumentiert.

Hazard	Situation			Hazard Impact	S	Severity	E	Exposure	C	Controlability	Risk rating
	Stand still	Forw. driving	Battery Full								
Function1: Positive Torque											
unintended positive torque	✓	-	-	Unintended forward vehicle movement	S3	It may affect a close passenger or pedestrian	E3	Stand still and pedastrians near by	C3	Not controllable	C
	×	✓	-	Acceleration instead of deceleration	S3	Collision with other car, getting off the road	E4	Highway driving or city driving	C2	Driver can still brake and steer with independent braking system	C
	×	×	×	unintended recuperation, driving slower backwards than expected	S0	No injuries	E4	Driving backwards is typical use condition for a car	C0	No special reaction necessary	QM
	×	×	✓	overcharging of battery, driving slower backwards than expected	S3	Fire or explosion of battery caused by overcharging	E1	Driving down a hill backwards is not a common situation	C3	Driver might not detect the error and cannot control it	A
More positive torque	×	-	-	Unintended vehicle acceleration	S3	Collision with other car, getting off the road	E4	Highway driving or city driving	C2	Driver can still brake and steer with independent braking system	C
No/less positive torque	-	-	-								QM

Abbildung 1: Auszug der "Hazard Analysis" und des „Risk Assessments"

Hazardous Event	ASIL	Safety Goal
Unintended positive torque while stand still	C	Avoid unintended positive torque at stand still
Unintended positive torque while driving forward	C	Avoid unintended positive torque while driving forward
Unintended positive torque while driving backwards with battery full	A	Avoid overcharging of battery
More positive torque while driving	C	Avoid torque above VCU request
Unintended negative torque while stand still	C	Avoid unintended negative torque at stand still
unintended negative torque during forward driving	C	Avoid unintended negative torque while driving forward
Unintended negative torque while driving backwards	C	Avoid unintended negative torque while driving backwards
Unintended negative torque while driving forward with battery full	A	Avoid overcharging of battery
More negative torque	B	Avoid torque below VCU request

Abbildung 2: Auszug der „Safety Goal Identifikation"

Component	Malfunction	Causing Faults	Safety Goal: Avoid unintended torque at stand still (no vehicle forward movement while standing still)	Allocated to	Driver warning
MAIN_SWITCH	no_hv_power	Batteriehauptschalter öffnet	no effect while standing still		
IGBT 18x 3teilsysteme	igbt_short	IGBT/Diode Kurzschluss	detect wrong signal with current and position sensor and establish ASC for the defect B6-Half-Bridge (the others stay active and allow limp-home)	ECU (detect and create PWM so that ASC is established)	Service Warning
IGBT	igbt_open	IGBT offen (Bonddraht)	no effect while standing still		
IGBT	wrong signal generated	Diode offen (Bonddraht)	no effect while standing still		
MOTOR	wrong_torque, too_much_heat (evtl zero_torque)	Windungskurzschluss	no effect while standing still		
CONTROLLER	no_mu_signal,		no effect while standing still (all IGBTS open)		
CONTROLLER	wrong_mu_signal	Steuerung fällt aus (Micorcontroller)	detect controller faults and mitigate or go to safestate (ASC)	ECU (detect), ECU (action: cut off PWM)	if mitigation fails indicate failure to driver
IGBT DRIVER 9x (SG2: IGBT)	igtb_driver_signal_open	Fehler IGBT Treiber (open) wie IGBT offen	no effect while standing still		Service Warning (if wrong signal)

Abbildung 3: Auszug aus dem "Functional Safety Concept"

Aufbauend auf dem ("Functional Safety Concept" (FSC)) wurden zum einen eine formale Safety Analyse angewandt, um konzeptionelle Fehler zu identifizieren bzw. auszuschließen. Dabei lag der Fokus auf der Erkennung von „Single Point of Failures" also der Erkennung von Schwachstellen im Sicherheitskonzept, die beim Ausfall einer einzelnen Komponente oder eines einzelnen Schutzmechanismus eine Bedrohung darstellen.

Zur Durchführung der formalen Analyse mit denen von OFFIS entwickelten Werkzeugen wurde zunächst eine Formalisierung der Anforderungen des Safety Konzepts durchgeführt. Abbildung 4 zeigt eine beispielhafte Formalisierung einer Anforderung, die im Wesentlichen aus einer Annahme und einer Zusicherung besteht. Die formalisierten Anforderungen werden über einen speziellen Editor eingegeben, der in Abbildung 5 dargestellt ist. Der Editor bietet dazu eine Auswahl möglicher Pattern und führt bei der Eingabe eine Syntaxüberprüfung durch.

IGBT Fault Propagation	
Assumption	`none of {{Controller_fail},{HV_fail}} does not occur`
Promise	`{!IGBTDM_nominal} does not occur`
Description	If there is no fault in the cointroller and no fault in the HV_power, the IGBTs are in nominal state.
Degradation Modes Order	IGBTDM_nominal -> IGBTDM_undetected -> Safestate

Abbildung 4: Beispielhafte Formalisierung einer funktionalen Sicherheitsanforderung

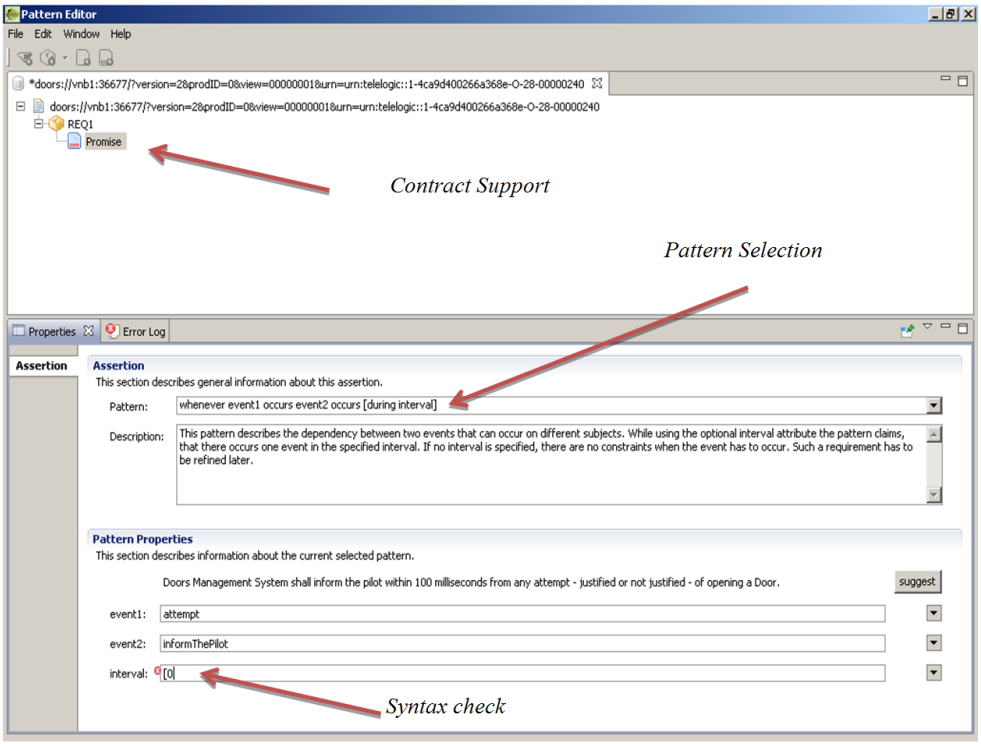

Abbildung 5: Editor zur Formalisierung der funktionalen Sicherheitsanforderungen

Nach der Eingabe der Anforderungen im Editor wird die formale Analyse durchgeführt. Diese überprüft ob ein sogenanntes Top-Level-Contract durch die Safety Requirements verletzt werden kann oder nicht. Im Fall der durchgeführten Analyse entsprach das Top-Level-Contract, wie oben bereits erläutert, der Frage nach der erfolgreichen Umsetzung von Redundanz im Sicherheitskonzept.

Abbildung 6 zeigt die formale Analyse mit dem positiven Validationsergebnis.

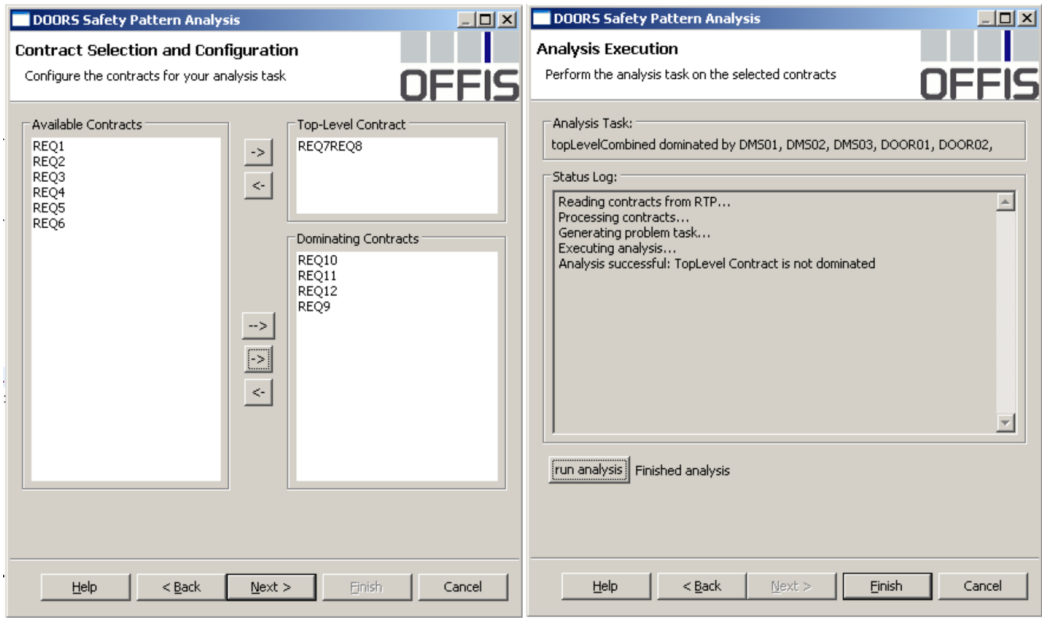

Abbildung 6: Formale Analyse zur Überprüfung eines Top-Level Contracts

Neben einer formellen Validierung wurde das funktionale Sicherheitskonzept zu einem technischen Sicherheitskonzepts („Technical Safety Concept“ (TSR)) entsprechend der ISO26262 verfeinert mit dem Ziel konkrete Anforderungen an die Umsetzung der Software und Hardware abzuleiten. Abbildung 7 zeigt einen Ausschnitt aus den technischen Sicherheitsanforderungen, deren ASIL Klassifikationen, der

Zuordnung zu Komponenten sowie der Unterscheidung zwischen Anforderungen an die Entwicklung von Hardware und Software.

ID	Refines	Requirement	ASIL	Rational	Component	HW/SW
TSR_001	FSR_005	Detect the overvoltage with a dedicated sensor	C		DC_LINK_SENSOR	HW
TSR_002	FSR_018	Evaluate information from dc_link_sensor in the controller and create ASC of the system	C		ECU	SW
TSR_003	FSR_101	Sensor shall read position of the rotor	A(C)		POSITION_SENSOR	HW
TSR_004	FSR_101	Controller needs to read position sensor and provide data to motor control task	A(C)		ECU	SW
TSR_005	FSR_102	Compute a simulation model of the motor in the controller	B(C)		ECU	SW
TSR_006	FSR_102	Compare position sensor values with the simulated model and switch to ASC of the system if values deviate.	B(C)		ECU	SW
TSR_007	FSR_103	IGBT Driver shall generate as output signal according to the PWM input	A(C)		IGBT Driver	HW
TSR_008	FSR_103	IGBT shall switch HV to the motor according to the input signal from the IGBT driver	A(C)		IGBT	HW
TSR_009	FSR_104	Compute a simulation model of the motor in the controller	B(C)		ECU	SW
TSR_010	FSR_104	If faults in one of the IGBTs is detected using the motor simulation model, establish ASC for the defect B6-Half-Bridge (the others stay active and allow limp-home)	B(C)		ECU	SW
TSR_011	FSR_105	A sensor shall measure the current at each of the phases of the motor	A(C)		CURRENT_SENSOR	HW

Abbildung 7: Technische Sicherheitsanforderungen (TSR)

In einem letzten Schritt wurden die technischen Sicherheitsanforderungen zu Anforderungen verfeinert, die konkrete Anforderungen an die Entwickler der jeweiligen SW Komponenten darstellen. Abbildung 8 zeigt beispielhaft, wie eine Anforderung an die Überwachung von Sensorwerten und der Reaktion im Falle eines Fehlers in Form eines aktiven Kurzschlusses in dedizierte Anforderungen an die Softwarekomponenten „Calibration“, „Monitoring“ und „Voter“ überführt wird.

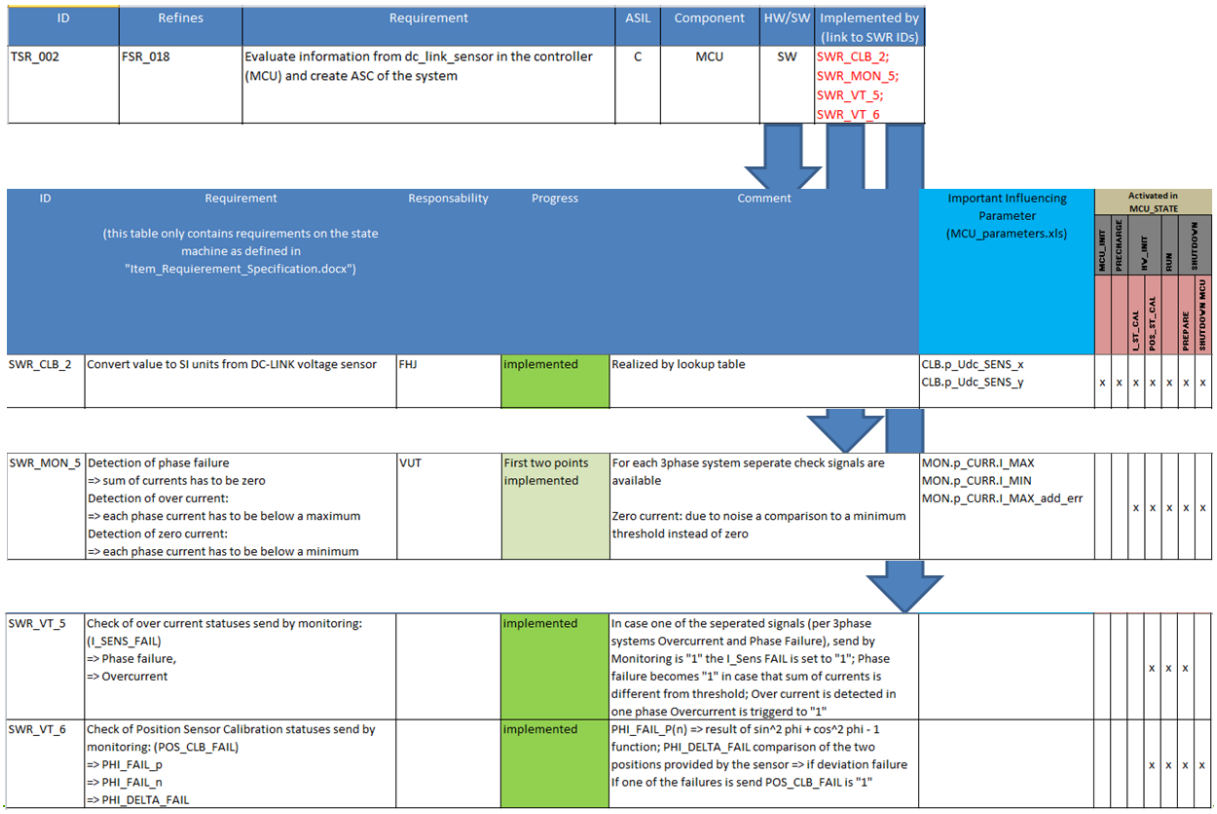

Abbildung 8: Beispielhafte Verfeinerung der technischen Safety Anforderungen zu Anforderungen an die Softwareentwicklung

Damit wurde in Arbeitspaket 2 die gesamte Entwicklung des Safety-Konzeptes beschrieben, wie sie nach der ISO26262 durchgeführt wurde. Zu jeder Zeit wurde dabei auf eine Zurückführbarkeit auf die übergeordneten Safety-Goals geachtet.

OFFIS hat diesen Prozess maßgeblich gesteuert und hat für die formale Analyse wissenschaftliche Methoden angewandt, die in derzeit laufende Standardisierungsaktivitäten in AUTOSAR münden.

Die Umsetzung der letztlich abgeleiteten Anforderungen an die Softwareentwicklung ist Bestandteil von Arbeitspaket 3 und wird von beteiligten Projektpartnern realisiert.

Arbeitspaket 3: "Brain- Safety critical control architectures"

In diesem Arbeitspakte wurde eine Toolchain aufgesetzt, die es ermöglicht, ausführbare Simulink Modelle in ein Funktionsnetzwerk zu überführen, um Realzeit-Eigenschaften des zugrundeliegenden Systems zu überprüfen. Diese Realzeit-Eigenschaften wurden im Rahmen des Safety-Konzepts definiert. Das Transformationsverfahren wurde zudem bereits mit verfügbaren Teilen des Motormodells getestet, die im Projekt bereits von Partnern zur Verfügung gestellt wurden. Die folgende Abbildung zeigt die Visualisierung eines Funktionsnetzwerkes, das aus Simulink über das Common Meta Model (CMM) Zwischenformat heraus erzeugt wurde.

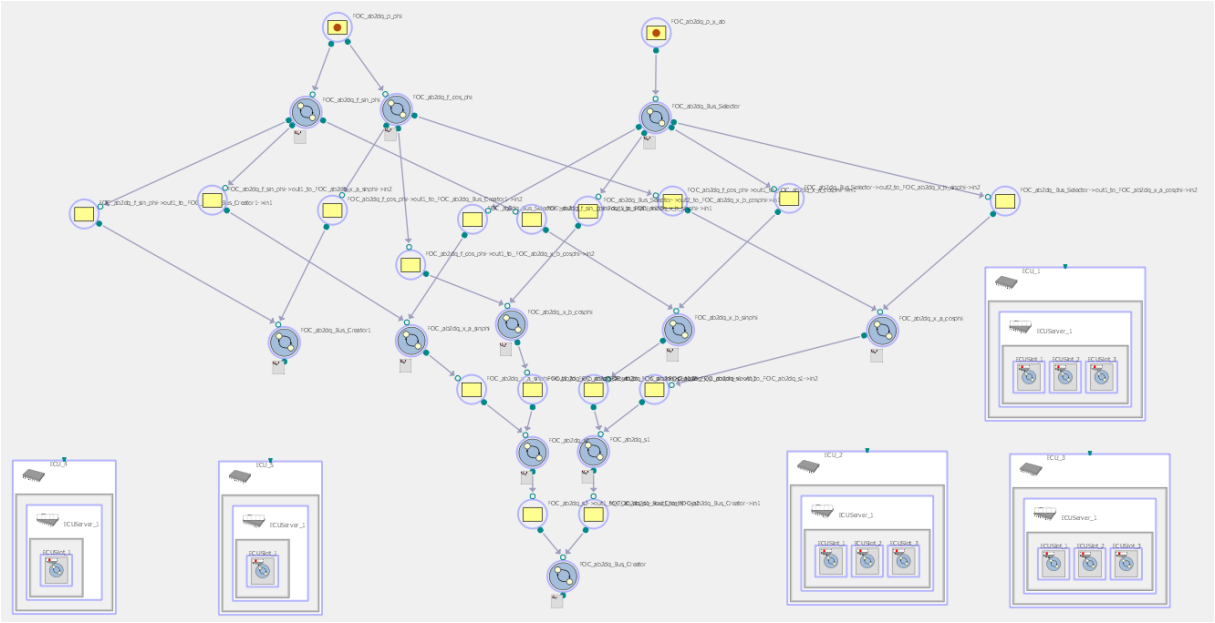

Abbildung 9: Funktionsnetzwerk für einen kleinen Ausschnitt der Motorsteuerung

Im nachfolgenden Schritt wurde dieses Analyseverfahren auf die gesamte Motorsteuerung angewandt, die von Projektpartnern entwickelt wurde. Abbildung 9 zeigt das resultierende Funktionsnetzwerk, das im Modellierungs- und Visualisierungswerkzeug Orca entstanden ist. Auf der rechten Seite sind die 3 Prozessorkerne des Aurix Multi-core Prozessors dargestellt, auf die die unterschiedlichen Softwaretasks abgebildet sind, wie es dem realen SW-Mapping in der Motorsteuerung entspricht.

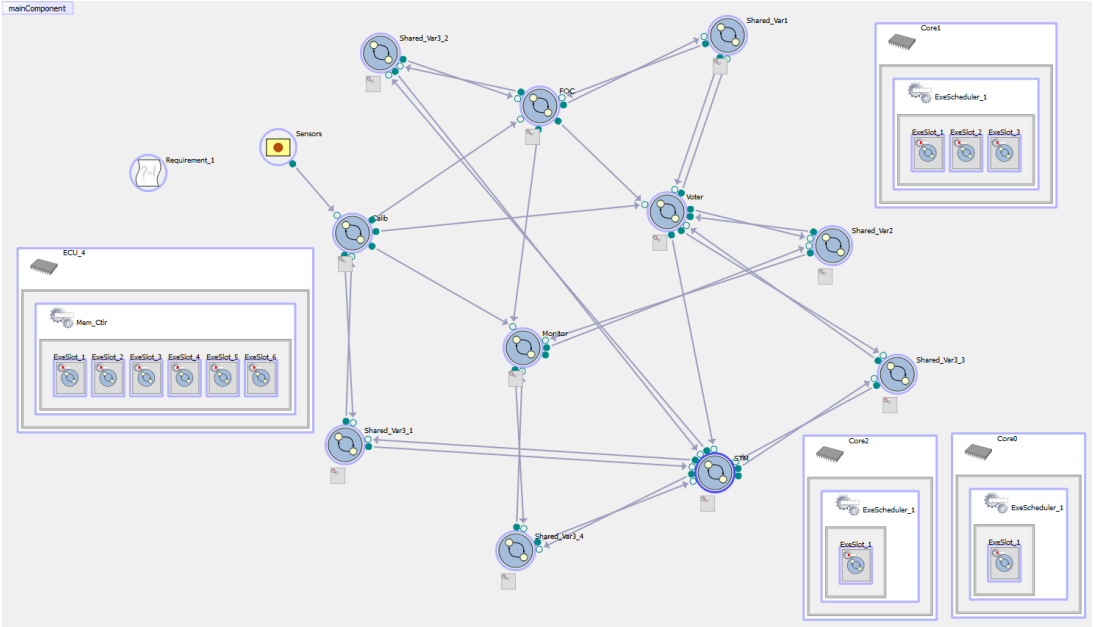

Abbildung 10: Orca Function Network Model

An dieses Funktionsnetzwerk wurden die Ausführungszeiten auf Task-Ebene sowie Zeiten für notwendige Kommunikationen zwischen den Kernen annotiert. Die Ausführungszeiten wurden dabei auf Grundlage von Simulationen gewonnen, die auf der virtuellen Plattform des Aurix-Controllers durchgeführt wurden. Das grundlegende Verfahren hierzu wurde in [P1] veröffentlicht. Darauf aufbauend wurde in [P4] die Ausführungszeitmessung für die im Projekt entwickelte Motorsteuerung im Detail vorgestellt.

Auf Grundlage dieses zeitannotierten Funktionsnetzwerkes wurde eine Analyse mit UPPAAL durchgeführt. Diese prüft formell und statisch verschiedene Systemeigenschaften. Zum einen ist dies die Einhaltung von Echtzeitanforderungen. Im konkreten Beispiel wurde die Deadline von 100µs für einen vollständigen Motorsteuerungszyklus überprüft. Des Weiteren wurde überprüft ob Deadlocks vorliegen, d.h. ob sich im System in einen Zustand begeben kann, der eine weitere Programmausführung blockiert. Abbildung 11 zeigt die formelle Analyse in UPPAAL. Es ist zu erkennen, dass sowohl die Echtzeitanforderungen erfüllt als auch Deadlocks ausgeschlossen wurden. Als dritte überprüfte Eigenschaft wurden Buffer Overflows ausgeschlossen.

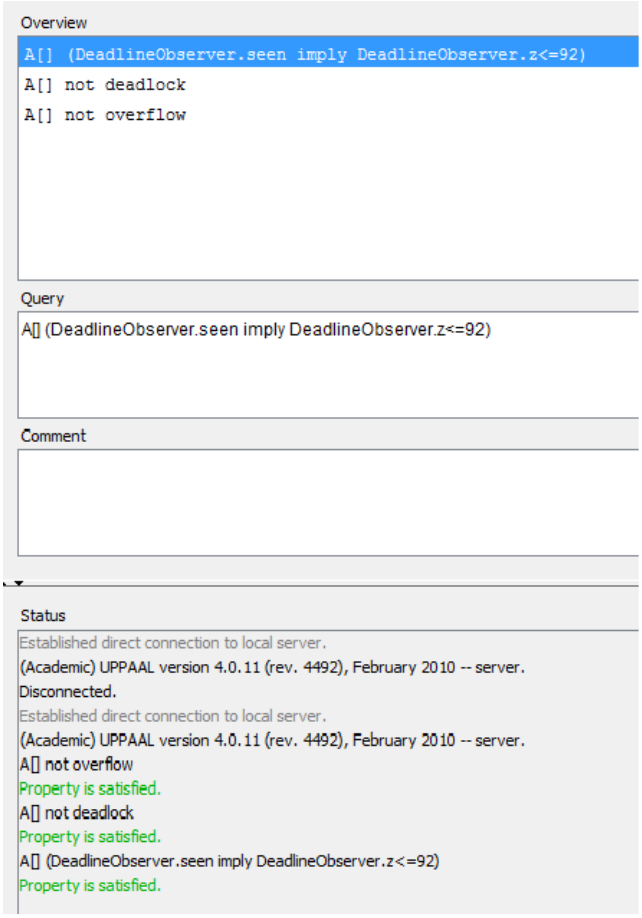

Abbildung 11: UPPAAL Realtime Analyse

Darüber hinaus wurde das in Arbeitspaket 1 erarbeitete Konzept zur Integration zur virtuellen Modellierung und Simulation (Virtual hardware in the loop (VPIL)) [P1] in die von Infineon zur Verfügung gestellte virtuelle Plattform des Multi-Core-Controllers (Infineon TriCore TC27x (AURIX)) umgesetzt [P4]. Dies beinhaltet das Aufsetzen der eigentlichen Plattform sowie spezifische Anpassungen der Hardware-Komponenten zur Umsetzung des Datenaustausches für die Co-Simulation mit Matlab Simulink (siehe Abbildung 12).

Mit Hilfe der VPIL Simulation konnten die zeitlichen und funktionalen Eigenschaften der Motorsteuerung validiert werden. Abbildung 13 zeigt die funktionalen Verifikationsergebnisse der VPIL Simulation für ein gegebenes Szenario, indem das angeforderte Drehmoment auf 50 Nm ausgelöst wird. Die Simulation von 10000 Steuerungsschritte (1 sec Simulationszeit) mit einem Abtastrate von 100 µs hat 944 s (15,7 min) gedauert. Das heißt, wir brauchen 15 Minuten für jeden Testfall, was eine angemessene Dauer ist unter der Berücksichtigung, dass das virtuelle Plattformmodell taktzyklusgenau arbeitet. Die Messwerte sind in Abbildung 13 zusammen mit den Simulationswerten des Simulink-Referenzmodells aufgetragen, wobei hier nur die Ausgänge der FOC-Komponente betrachtet wurden. Das Referenzmodell der FOC Aktorwerte (gestrichelte Linie) und die gemessenen Aktorwerte (dicke durchgezogene Linie) zeigen genau die gleichen Ergebnissen. Somit wird die Funktionalität des erzeugten Codes auf der betrachteten Multicore-Plattform erfolgreich gegen das Referenzmodell in Simulink (für das gegebene Szenario) überprüft.

Andere Szenarien, bereitgestellt vom Projektpartner FH Johanneum, wurden in gleicher Weise validiert.

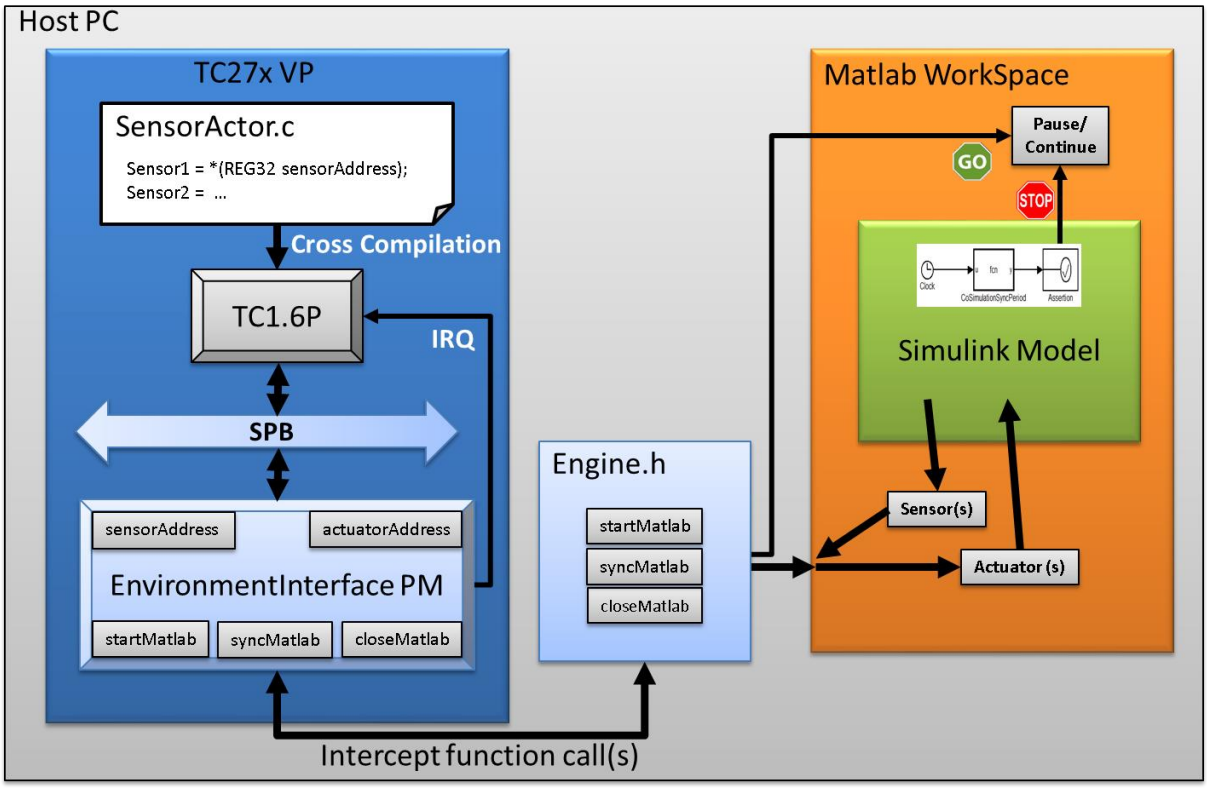

Abbildung 12: Virtual hardware in the loop (VPIL)

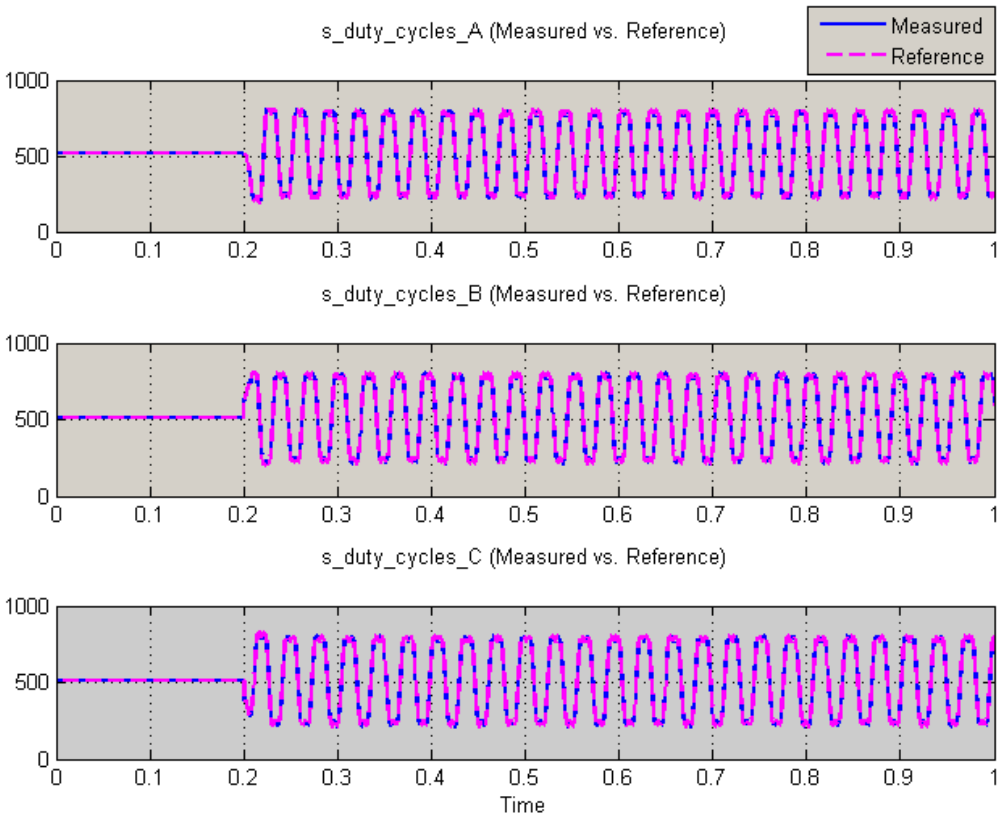

Abbildung 13: VPIL funktionale Validierung (für eine Drehmomentanforderung von 50Nm)

Zudem wurde ein Konzept entwickelt, wie ein in Simulink spezifiziertes Modell auf einer Multi-Core Plattform formal bezüglich Echtzeitanforderungen analysiert werden kann. Im Gegensatz zu bisherigen Ansätzen, wird hierbei eine deutlich höhere Genauigkeit (durch geringere Überapproximation) erreicht, wodurch die Zeitabschätzungen deutlich näher an den tatsächlichen Ergebnissen liegen und damit weniger pessimistisch sind. Eine detaillierte Beschreibung des Konzepts wurde auf der DATE 2013 Konferenz vorgestellt [P2]. Eine Erweiterung unseres Ansatzes wurde in [P3] vorgestellt. Dies ermöglicht die zeitliche Analyse einer größeren Anzahl von Applikationen als in [P2] betrachtet werden konnten.

In Unterschied der oben dargestellten funktionsnetzwerkebasierten Echtzeitanalyse, setzt dieses neue Konzept darauf Simulink Modelle als Synchrone Datenflussgraphen (SDFG) zu repräsentieren (siehe Abbildung 14). SDF Graphen haben den Vorteil, dass sie aufgrund ihrer einfacheren Semantik besser skalieren als andere (ausdrucksmächtigere) Ansätze. Diese Methode wurde auf den von uns betrachteten MotorBrain Anwendungsfall (ähnlich wie oben bei der funktionsnetzwerkbasierten Echtzeitanalyse) angewandt. Der Nachweis der besseren Skalierbarkeit könnte nachgewiesen werden (siehe [P4, P7]).

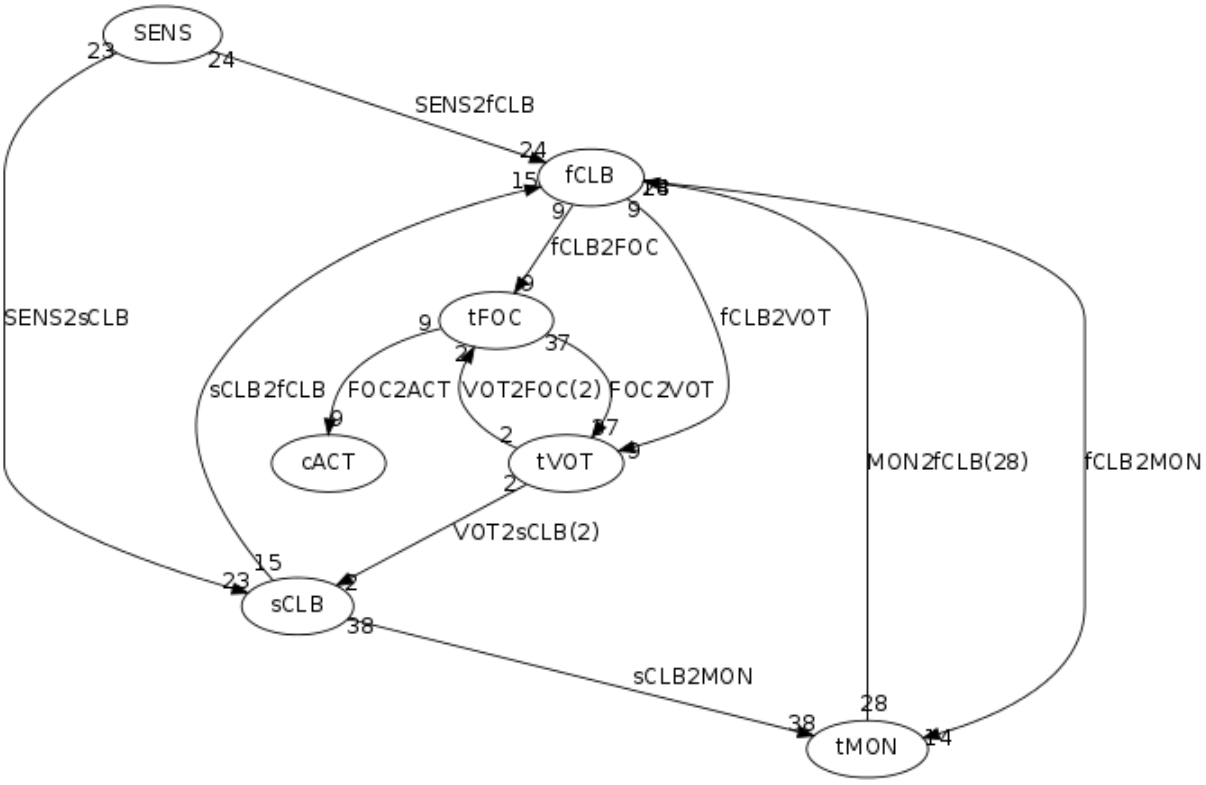

Abbildung 14: Motorsteuerung Synchrone-Datenfluss Graphen

Arbeitspaket 6: „EV integration and demonstrations“

Im Rahmen diese Arbeitspakets hat OFFIS das im Projekt entstandene Motor-Steuergerät mit einem (virtuellen) Modell des Motorverhaltens integriert, um ein frühes Testen der Steuerungssoftware in Bezug auf zeitliches und funktionales Verhalten sowie der Reaktion auf injizierte Fehler zu ermöglichen. Die Vorteile dieser Hardware-in-the-Loop (HIL) Simulation gegenüber des Testens mit realem Motor sind vielfältig: die Validation kann deutlich früher starten da der entwickelte Motor erst zu einem späteren Zeitpunkt im Projekt zur Verfügung steht, die entwickelte Testumgebung ist echtzeitfähig sowie besonders günstig und sie erfordert keine aufwändige Inbetriebnahme des Motors auf dem Teststand.

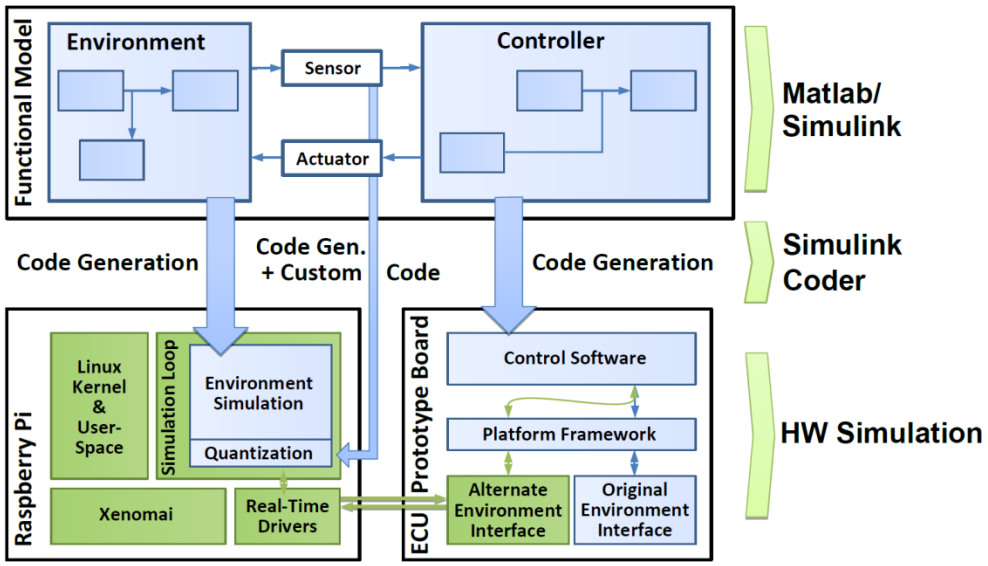

Abbildung 15: Konzept der virtuellen Integration und Echtzeit-Simulation

Die Architektur der entwickelten Echtzeitsimulation ist in Abbildung 15 dargestellt. Ausgangspunkt sind die funktionalen Modelle der Motorsteuerung und dessen Umwelt (Motor und Sensorik) als Matlab/Simulink Modell. Für die Motorsteuerung wurde eine Codeerzeugung mittels Simulink Coder durchgeführt, die Anwendung wird für die Zielplattform (Infineon Aurix TriCore) kompiliert und dort zur Ausführung gebracht. Das Motorverhalten wird ebenfalls vom Matlab/Simulink Modell mittels Codeerzeugung in eine lauffähige Anwendung überführt, die auf einer günstigen Hardwareplattform (Raspberry Pi) zur Ausführung gebracht wurde. Auf dem Raspberry Pi läuft das Motorverhalten als Programm innerhalb eines Echtzeit Linux Betriebssystems. Der Raspberry Pi emuliert dabei in Echtzeit einen realen Motor und kommuniziert mit dem Motor Steuergerät auf ähnlichem Wege wie es ein realer Motor tun würde. Eine detaillierte Beschreibung der entwickelten Echtzeitsimulation wurde in [P5, P6] veröffentlicht.

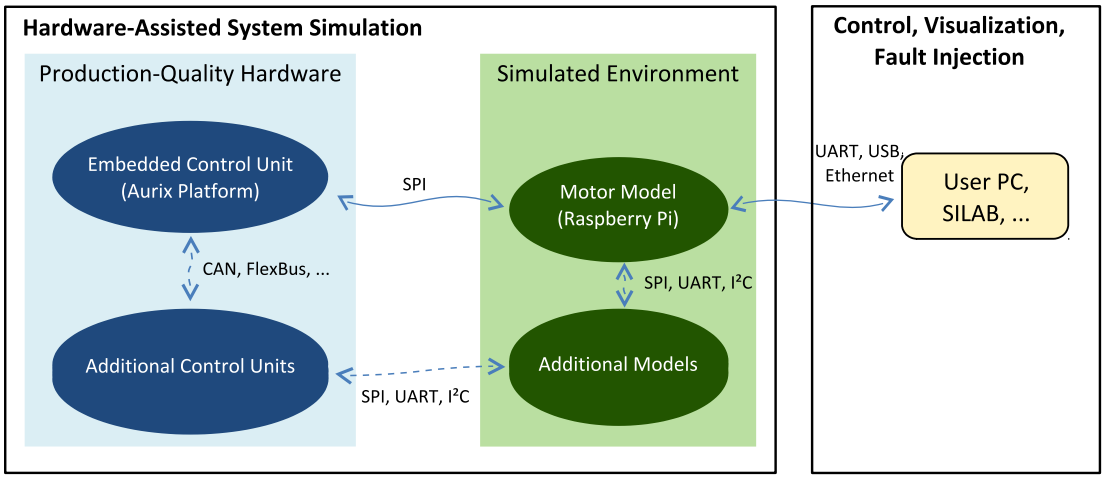

Abbildung 16: Hardwaregestützte Simulation

Als weitere Komponente wurde eine Verbindung zu einem PC hergestellt, der in erster Linie als Debug- und Visualisierungskonsole dient. Abbildung 16 zeigt die eingesetzten Schnittstellen innerhalb der HIL Simulation und zwischen Raspberry Pi und PC.

Abbildung 17 zeigt die Visualisierung der Motorphasen bei verschiedenen Lastgängen, die sich über den PC einstellen lassen, was zum Beispiel verschiedenen Steigungen entspricht.

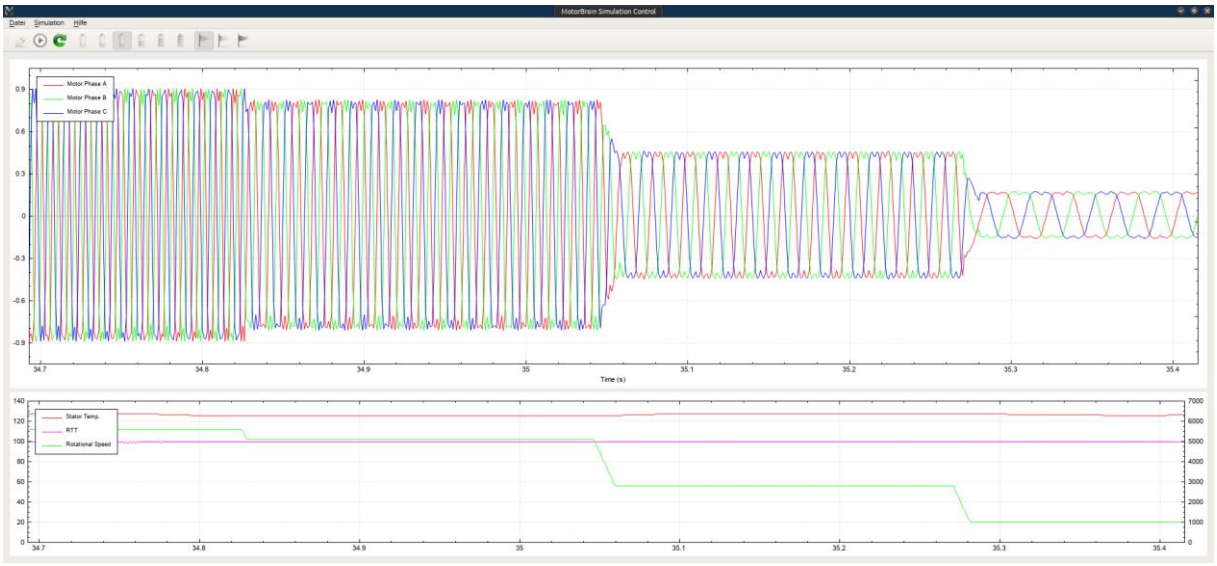

Abbildung 17: Visualisierung der Motorphasen bei verschiedenen Lastgängen

Der vollständige Aufbau des HIL Demonstrators ist in Abbildung 18 dargestellt. Auf der linken Seite ist das Steuergerät zu sehen, das über die SPI Schnittstelle mit dem Raspberry Pi auf der rechten Seite verbunden ist.

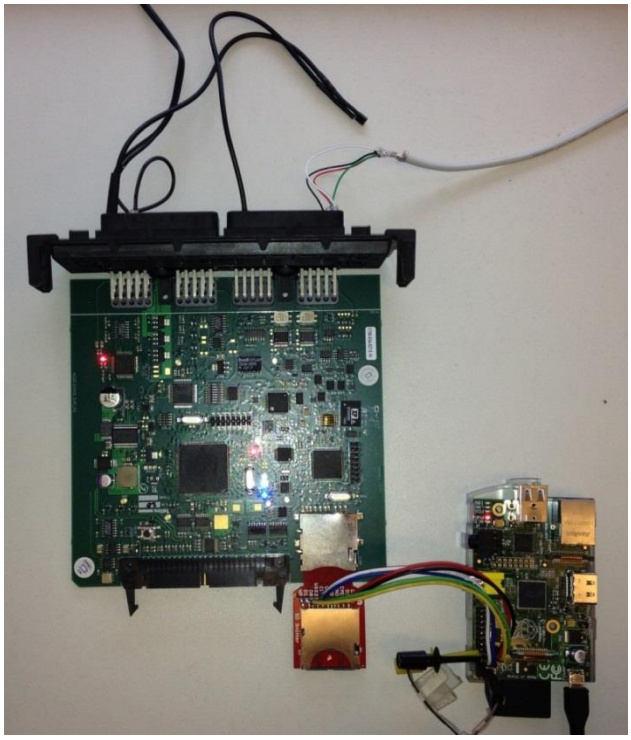

Abbildung 18: Aufbau der HIL Simulation

II.2 Voraussichtlicher Nutzen

Sicherheitsanalysen und Zertifizierungsprozesse in der Automobilindustrie werden durch zukünftige Entwicklungen und eine weitere Erhöhung des Softwareanteils an sicherheitskritischen Steuerungen (vollelektrischer Antriebsstrang, teilweise und vollständig automatisches Fahren), werden aufwendiger und kostenintensiver. OFFIS hat diese Themen in MotorBrain vorranging behandelt und brachte vorhandene Spezifikationstechniken, Analysetechniken und Know-How zu Zertifizierungsprozessen in das Projekt. Die in anderen Projekten entwickelten Tools und Erfahrungen konnten auf der einen Seite den MotorBrain Industriepartnern zur Verfügung gestellt werden, auf der

anderen Seiten können sie notwenigen Verbesserungen (die im Rahmen der Kooperation in Motorbrain entstehen) in die Tools und Methoden eingebracht werden. Die beteiligten deutschen Industriepartner (in SC2 und SC8) werden die vorgeschlagene Vorgehensweisen zum, Entwurf, zur Implementierung und zur Integration verwenden, um sich damit einen Wettbewerbsvorteil gegenüber den Konkurrenten auf dem Weltmarkt zu sichern. Darüber hinaus hat OFFIS die Teilnahme an dem MotorBrain Projekt einen interdisziplinären Einblick in die Entwicklung moderner vollelektrischer Antriebsstränge ermöglicht, den wir ohne diese Projektbeteiligung in dieser thematischen Breite nicht erhalten hätten. Dieses neue Wissen und die daraus entstandenen Partnerschaften ermöglichen uns auch in zukünftigen Projekten die Zusammenarbeit mit Partnern in dieser Anwendungsdomäne. Als unmittelbare Nachfolgeaktivität hat sich die Beteiligung an dem Europäischen 3CCar Project (ECSEL) ergaben. Hier wird aufbauend auf den MotorBrain-Aktivtäten und Ergebnissen an ausfallsicheren vollelektrischen Antriebsstränge geforscht.

Einige der Themen dienen als Grundlage für zukünftige und gegenwärtige Dissertationen: „State-Based Real-Time Analysis of SDF Applications on MPSoCs with Shared Communication Resources“ von Maher Fakih und „Change Impact Analysis for Safety-critical Embedded Systems“ von Markus Oertel.

II.3 Bekannt gewordener Fortschritt bei anderen Stellen

Vor kurzem wurde ein Ansatz in [1] vorgestellt, welcher Model-Checking mit dem Real-time Calculus vereint, um die Skalierbarkeit der Worst-Case Antwortzeitanalyse für Multicores zu verbessern. Tasks werden in einer sog. Superblockdarstellung repräsentiert, in welcher Ressourcenzugriffsphasen leicht identifiziert werden können. In unserer Arbeit hingegen konzentrieren wir uns auf SDF-basierte Anwendungen mit ihren spezifischen Eigenschaften und Bedingungen. Wir betrachten auch ein weniger abstrahiertes System-Modell als das in [1] vorgestellte, wo wir Blockierung bei gemeinsamen FIFO-Puffern, Multi-Port Akteure und ein hierarchisches Scheduling zwischen verschiedenen Anwendungen betrachten. Dennoch ist es möglich, die in [1] vorgestellten Abstraktionstechniken zu nutzen um damit auch SDF-Anwendungen zu analysieren.

Unsere in MotorBrain durchgeführten Arbeiten zur Übersetzung von SDFGs zu Realzeitautomaten sind die ersten in der Literatur bekannt gewordenen Arbeiten, um Echtzeiteigenschaften Eigenschaften von auf MPSoCs abgebildeten SDFGs mit Hilfe von Model-Checking zu analysieren. Unser Ansatz wurde später von anderen Forschern in [2, 3, 4] übernommen, um SDFGs/SADGs mit Hilfe von Model-Checking zu analysieren.

In [2] wird eine Übersetzung der einzelnen SDFGs zu Realzeitautomaten beschrieben, um ihr Verhalten mit Model-Checking zu analysieren. Im Gegensatz zu unserer Arbeit, konzentrierten sich die Autoren dieser Arbeit auf die Suche nach einem maximalen (Token/Daten-)Durchsatz für eine gegebene Anzahl von Prozessoren.

Die Autoren von [3] übersetzen ein Systemmodell, welches (wie auch in unserer Arbeit) einen SDFG und dessen Abbildung auf eine Multiprozessorplattform enthält, in ein Netzwerk von sogenannten Priced Timed-Automaten und nutzen einen erweiterten Model-Checker, um ein optimales Scheduling mit optimalem Durchsatz und Energieverbrauch zu erhalten.

Vor kurzem präsentierten die Autoren von [4] eine Übersetzung von Finite-State-Maschine-Scenario-aware-Data-Flow (FSM-SADF) Graphen zu Timed Automaten. FSM-SADF ist ein Berechnungsmodell das ausdrucksstärker als SDF ist (aber damit andere Einschränkungen bzgl. der Analysierbarkeit mit sich bringt). Ähnlich wie bei unserer Arbeit, nutzten die Autoren Model-Checking auf FSM-SADFs um komplexe Eigenschaften nachzuweisen, die von traditionellen Werkzeugen (wie z.B. SDF3) in der Analyse nicht unterstützt werden.

Nach bestem Wissen sind uns keine weiteren Ansätze bekannt, die Model-Checking für die Zeitvalidierung von mehreren harten Echtzeit-SDFGs unter der Abbildung auf ein Multiprozessor-System-on-Chip (MPSoC), unter Nutzung gemeinsamer geteilter On-Chip-Kommunikationsressourcen

(Busse, DMA), mit der Unterstützung unterschiedlicher Arbitrierungsprotokolle (z.B. First-come-First-Serve (FCFS), Round-Robin (RR), fester Priorität (FP) und Time Division Multiple Access (TDMA)) vorgeschlagen haben oder benutzen.

II.4 Veröffentlichungen

[P1] M. Fakih und K. Grüttner: "Virtual–Platform in the Loop Simulation for Accurate Timing Analysis of Embedded Software on Multicore Platforms", in *ASIM–Konferenz STS/GMMS 2012*, Shaker Verlag.

[P2] M. Fakih, K. Grüttner, M. Fränzle und R. Rettberg: "Towards Performance Analysis of SDFGs Mapped to Shared–Bus Architectures Using Model–Checking", in *Proceedings of the Conference on Design, Automation and Test in Europe (DATE) 2013*, European Design and Automation Association, 3001 Leuven, Belgium, Belgium.

[P3] M. Fakih, K. Grüttner, M. Fränzle und A. Rettberg; "Exploiting Segregation in Bus–Based MPSoCs to Improve Scalability of Model–Checking–Based Performance Analysis for SDFAs", in *Proceedings of* the *International Embedded Systems Symposium (IESS)* 2013.

[P4] M. Fakih, K. Grüttner, M. Fränzle und A. Rettberg: „Multicore Performance analysis of a Multi–phase Electrical Motor Controller", in *Proceedings of the Embedded Real Time Software and Systems Congress (ERTS2)* 2014.

[P5] S. Rosinger, M. Fakih und J. Walter: "MOTORBRAIN: Model-based Design and Virtual-Integration of an Intelligent and Safe Electrical Powertrain", *Conference on Design, Automation and Test in Europe (DATE) 2014 - University Booth*.

[P6] J. Walter, M. Fakih und K. Grüttner: "Hardware–Based Real–Time Simulation on the Raspberry Pi", in *Workshop on High-performance and real-time embedded systems (HiRES)*, HiPEAC conference 2014.

[P7] M. Fakih, K. Grüttner, M. Fränzle und A. Rettberg: "State-Based Real-Time Analysis of SDF Applications on MPSoCs with Shared Communication Resources", *Journal of Systems Architecture*, 1383-7621 (to appear).

III. Referenzen

[1] Georgia Giannopoulou, Kai Lampka, Nikolay Stoimenov, and Lothar Thiele. Timed model checking with abstractions: Towards worst-case response time analysis in resource-sharing manycore systems. In Proc. International Conference on Embedded Software (EMSOFT), pages 63–72, Tampere, Finland, Oct 2012. ACM.

[2] W. Ahmad, E. de Groote, P.F.K. Hölzenspies, M.I.A. Stoelinga, and J.C. van de Pol. Resource-constrained optimal scheduling of synchronous dataflow graphs via timed automata. In Proceedings of 14th IEEE International Conference on Application of Concurrency to System Design (ACSD). IEEE, 2014.

[3] Xue-Yang Zhu, Rongjie Yan, Yu-Lei Gu, and Guangquan Zhang. Static Optimal Scheduling and Mapping of Synchronous Dataflow Graphs on a Heterogeneous Multiprocessor Platform with Model Checking. 2014.

[4] Mladen Skelin, Erik Ramsgaard Wognsen, Mads Chr. Olesen, Rene Rydhof Hansen, and Kim Guldstrand Larsen. Towards translating FSM-SADF to timed automata. In 1st International Workshop on Investigating Dataflow in Embedded computing Architecture (IDEA), 1 2015.

Berichtsblatt

1. ISBN oder ISSN 978-3-901608-39-1	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung

3. Titel
Virtual-Platform in the Loop Simulation for Accurate Timing Analysis of Embedded Software on Multicore Platforms

4. Autor(en) [Name(n), Vorname(n)] Fakih, Maher Grüttner, Kim	5. Abschlussdatum des Vorhabens 01.10.2014
	6. Veröffentlichungsdatum 24. Februar 2012
	7. Form der Publikation Artikel in Konferenzbericht
8. Durchführende Institution(en) (Name, Adresse) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N11480
	11. Seitenzahl 11
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 15
	14. Tabellen
	15. Abbildungen 5

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
GI ASIM Fachgruppen "Simulation technischer Systeme" (STS) und "Grundlagen und Methoden in Modellbildung und Simulation" (GMMS) Workshop
Wolfenbüttel 23. – 24. Februar 2012

18. Kurzfassung
The design of embedded systems with real time requirements is a challenging task. On one side, timing predictability is fundamental for guaranteeing safe system operation. On the other side, complex functional behavior needs to be validated at all refinement levels during the design. For multicore platforms this task becomes even more challenging due to the increased complexity in platform parallelism including access arbitration to shared resources such as memories or peripherals, which impact software execution times. This paper describes a co-simulation based validation method for embedded software implemented on multicore hardware platforms. The co-simulation is realized between Simulink and the SystemC-based SoCLib virtual-platform framework. Simulink is used to implement the system environment and functional model of an embedded control system. SoCLib is used to model a multicore execution platform with shared resources. Our design flow enables code generation and deployment from a Simulink model, and execution of this code on a multicore platform. In addition our virtual-platform model allows the observation of software execution and its timing measurement at a cycle accurate level. We demonstrate the applicability of our method through validation of a real-time critical ignition controller system by running our virtual multicore platform in the loop with the Simulink environmental model.

19. Schlagwörter

20. Verlag ARGESIM-Verl.	21. Preis

Berichtsblatt

1. ISBN oder ISSN 978-3-9815370-0-0	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung

3. Titel
Towards Performance Analysis of SDFGs Mapped to Shared-Bus Architectures Using Model-Checking

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens 01.10.2014
Maher Fakih, Kim Grüttner , Martin Fränzle, Achim Rettberg	6. Veröffentlichungsdatum 3/2013
	7. Form der Publikation Artikel in Konferenzbericht
8. Durchführende Institution(en) (Name, Adresse) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg Carl von Ossietzky University, Germany Ammerländer Heerstraße 114-118, 26129 Oldenburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N11480
	11. Seitenzahl 6
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 14
	14. Tabellen 4
	15. Abbildungen 5

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
Proceedings of the Conference on Design, Automation and Test in Europe (DATE)
3001 Leuven, Belgium, 3/2013

18. Kurzfassung

The timing predictability of embedded systems with hard real-time requirements is fundamental for guaranteeing their safe usage. With the emergence of multicore platforms this task became very challenging. In this paper, a model- checking based approach will be described which allows us to guarantee timing bounds of multiple Synchronous Data Flow Graphs (SDFG) running on shared-bus multicore architectures. Our approach utilizes Timed Automata (TA) as a common semantic model to represent software components (SDF actors) and hardware components of the multicore platform. These TA are explored using the UPPAAL model-checker for providing the timing guarantees. Our approach shows a significant precision improvement compared with the worst-case bounds estimated based on maximal delay for every bus access. Furthermore, scalability is examined to demonstrate analysis feasibility for small parallel systems.

19. Schlagwörter

20. Verlag European Design and Automation Association	21. Preis

Berichtsblatt

1. ISBN oder ISSN 978-3642388521	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung

3. Titel
Exploiting Segregation in Bus-Based MPSoCs to Improve Scalability of Model-Checking-Based Performance Analysis for SDFAs

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens 01.10.2014
Maher Fakih, Kim Grüttner, Martin Fränzle, Achim Rettberg	6. Veröffentlichungsdatum 06 / 2013
	7. Form der Publikation Artikel in Konferenzbericht
8. Durchführende Institution(en) (Name, Adresse) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg Carl von Ossietzky University, Germany Ammerländer Heerstraße 114-118, 26129 Oldenburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N11480
	11. Seitenzahl 13
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 16
	14. Tabellen 1
	15. Abbildungen 2

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
4th IFIP TC 10 International Embedded Systems Symposium, IESS 2013
Paderborn, Germany, 06 / 2013

18. Kurzfassung

The timing predictability of embedded systems with hard real-time requirements is fundamental for guaranteeing their safe usage. With the emergence of multicore platforms this task becomes even more challenging, because of shared processing, communication and memory resources. Model-checking techniques are capable of verifying the performance properties of applications running on these platforms. Unfortunately, these techniques are not scalable when analyzing systems with large number of tasks and processing units. In this paper, a model-checking based approach that allows to guarantee timing bounds of multiple Synchronous Data Flow Applications (SDFA) running on shared-bus multicore architectures will be extended for a TDMA hypervisor architecture. We will improve the the number of SDFAs being analyzable by our model-checking approach by exploiting the temporal and spatial segregation properties of the TDMA architecture and demonstrate how this method can be applied.

19. Schlagwörter

20. Verlag Springer; Auflage: 2013 (28. Juni 2013)	21. Preis

Berichtsblatt

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

3. Titel
Multicore Performance analysis of a Multi-phase Electrical Motor Controller

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens 01.10.2014
Maher Fakih, Kim Grüttner, Martin Fränzle, Achim Rettberg	6. Veröffentlichungsdatum 02 / 2014
	7. Form der Publikation Artikel in Konferenzbericht
8. Durchführende Institution(en) (Name, Adresse) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg Carl von Ossietzky University, Germany Ammerländer Heerstraße 114-118, 26129 Oldenburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N11480
	11. Seitenzahl 10
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 26
	14. Tabellen 0
	15. Abbildungen 8

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
International Conference on Embedded Real Time Software and Systems 2014 (ERTS²)
Toulousse, France 02 / 2014

18. Kurzfassung

The timing predictability of embedded systems with hard real-time requirements is fundamental for guaranteeing their safe usage. With the emergence of multicore platforms this task becomes even more challenging, because of shared processing, communication and memory resources. In this paper, a combination of simulative method with a performance analysis based on model-checking is proposed. The simulative approach is used for functional validation of the Synchronous Data Flow Application (SDFA) implementation and its mapping on the targeted hardware platform. In our proposed methodology, we are using a binary-compatible and cycle-accurate virtual platform representation to simulate and map all relevant architectural properties to our analytical performance model. In combination, the model-checking based method allows to guarantee timing bounds of multiple Synchronous Data Flow Application (SDFA) implementations. This approach utilizes Timed Automata (TA) as a common semantic model to represent WCET of software components (SDF actors) and access protocols including timing of shared buses, shared DMAs, private local and shared memories of the multicore platform. The resulting network of TA is analyzed using the UPPAAL model-checker for providing safe timing bounds of the implementation. We demonstrate our approach using a multi-phase electric motor control algorithm (modeled as SDFA) mapped to Infineon's TriCore-based Aurix multicore hardware platform.

19. Schlagwörter

20. Verlag Proceedings of ERTS² 2014	21. Preis

Berichtsblatt

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

3. Titel
Hardware-Based Real-Time Simulation on the Raspberry Pi

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens 01.10.2014
Walter, Jörg Fakih, Maher Grüttner, Kim	6. Veröffentlichungsdatum 01 / 2014
	7. Form der Publikation Artikel in Konferenzbericht
8. Durchführende Institution(en) (Name, Adresse) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N11480
	11. Seitenzahl 12
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 22
	14. Tabellen 2
	15. Abbildungen 4

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
2nd Workshop on High-performance and Real-time Embedded Systems (HiRES 2014)
Vienna, Austria, January 20, 2014

18. Kurzfassung

Hardware prototypes are commonly used during embedded control unit design. Existing commercial tools offer an integrated workflow from mathematical models down to hardware simulation. Researchers also build low-cost simulation platforms out of commodity equipment. We present a platform that is an order of magnitude cheaper than existing systems but still easy to integrate into present workflows: Within an existing model-driven design methodology, we perform real-time hardware simulation using the Raspberry Pi single-board computer to simulate an electromechanical system with little development effort."

19. Schlagwörter

20. Verlag Proceedings of HiRES 2014	21. Preis

Berichtsblatt

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

3. Titel
Model-Based Design and Virtual Integration of an Intelligent and Safe Electrical Powertrain

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens 01.10.2014
Sven Rosinger, Maher Fakih Jörg Walter	6. Veröffentlichungsdatum 03 / 2014
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N11480
	11. Seitenzahl 1
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben
	14. Tabellen 1
	15. Abbildungen 5

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
Conference on Design, Automation and Test in Europe DATE'14 -University Booth
Dresden, Germany, 2014

18. Kurzfassung

19. Schlagwörter

20. Verlag	21. Preis

Berichtsblatt

1. ISBN oder ISSN 1383-7621	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung

3. Titel
State-Based Real-Time Analysis of SDF Applications on MPSoCs with Shared Communication Resources

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens
Maher Fakih, Kim Grüttner, Martin Fränzle, Achim Rettberg	6. Veröffentlichungsdatum To appear 05/2015
	7. Form der Publikation Journal Artikel
8. Durchführende Institution(en) (Name, Adresse) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg Carl von Ossietzky University, Germany Ammerländer Heerstraße 114-118, 26129 Oldenburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N11480
	11. Seitenzahl 28
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 42
	14. Tabellen 3
	15. Abbildungen 23

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
Journal of Systems Architecture (JSA) 2015

18. Kurzfassung

The timing predictability of Multi-Processor System on Chip (MPSoC) platforms with hard real-time applications is much more challenging than that of traditional platforms due to their large number of shared processing, communication and memory resources. Yet, this is an indispensable challenge for guaranteeing their safe usage in safety critical domains (avionics, automotive). In this article, a real-time analysis based on model-checking is proposed. The model-checking based method allows guaranteeing timing bounds of multiple Synchronous Data Flow Application (SDFA) implementations. This approach utilizes Timed Automata (TA) as a common semantic model to represent WCET of software components (SDF actors) and shared communication resource access protocols for buses, DMA, private local and shared memories of the MPSoC. The resulting network of TA is analyzed using the UPPAAL model-checker for providing safe timing bounds of the implementation. Furthermore, we will show the extension of our previous system model enabling single-beat inter-processor communication style beside the burst-transfer style and provide the implementation of the complete set of TA templates capturing the considered system model. We demonstrate our approach using a multi-phase electric motor control algorithm (modeled as SDFA) mapped to Infineon's TriCore-based Aurix multicore hardware platform with both the burst and single-beat inter-processor communication styles. Our approach shows a significant precision improvement (up to a percentage improvement of 300%) compared with the worst-case bound calculation based on a pessimistic analytical upper-bound delays for every shared resource access. In addition, scalability is examined to demonstrate analysis feasibility for small parallel systems, up to 40 actors mapped to 4-tiles and up to 96 actors on a 2-tiles platforms.

19. Schlagwörter

20. Verlag Journal of Systems Architecture	21. Preis

Document Control Sheet

1. ISBN or ISSN 978-3-901608-39-1	2. type of document (e.g. report, publication) publication
3. title Virtual-Platform in the Loop Simulation for Accurate Timing Analysis of Embedded Software on Multicore Platforms	
4. author(s) (family name, first name(s)) Fakih, Maher Grüttner, Kim	5. end of project 01.10.2014
	6. publication date 24. Februar 2012
	7. form of publication Inproceeding
8. performing organization(s) (name, address) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg	9. originator's report no.
	10. reference no. 13N11480
	11. no. of pages 11
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 15
	14. no. of tables
	15. no. of figures 5
16. supplementary notes	
17. presented at (title, place, date) GI ASIM Fachgruppen "Simulation technischer Systeme" (STS) und "Grundlagen und Methoden in Modellbildung und Simulation" (GMMS) Workshop Wolfenbüttel 23. – 24. Februar 2012	
18. abstract The design of embedded systems with real time requirements is a challenging task. On one side, timing predictability is fundamental for guaranteeing safe system operation. On the other side, complex functional behavior needs to be validated at all refinement levels during the design. For multicore platforms this task becomes even more challenging due to the increased complexity in platform parallelism including access arbitration to shared resources such as memories or peripherals, which impact software execution times. This paper describes a co-simulation based validation method for embedded software implemented on multicore hardware platforms. The co-simulation is realized between Simulink and the SystemC-based SoCLib virtual-platform framework. Simulink is used to implement the system environment and functional model of an embedded control system. SoCLib is used to model a multicore execution platform with shared resources. Our design flow enables code generation and deployment from a Simulink model, and execution of this code on a multicore platform. In addition our virtual-platform model allows the observation of software execution and its timing measurement at a cycle accurate level. We demonstrate the applicability of our method through validation of a real-time critical ignition controller system by running our virtual multicore platform in the loop with the Simulink environmental model.	
19. keywords	
20. publisher ARGESIM-Verl.	21. price

Document Control Sheet

1. ISBN or ISSN 978-3-9815370-0-0	2. type of document (e.g. report, publication) publication
3. title Towards Performance Analysis of SDFGs Mapped to Shared-Bus Architectures Using Model-Checking	
4. author(s) (family name, first name(s)) Maher Fakih, Kim Grüttner , Martin Fränzle, Achim Rettberg	5. end of project 01.10.2014 6. publication date 3/2013 7. form of publication Inproceeding
8. performing organization(s) (name, address) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg Carl von Ossietzky University, Germany Ammerländer Heerstraße 114-118, 26129 Oldenburg	9. originator's report no. 10. reference no. 13N11480 11. no. of pages 6
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 14 14. no. of tables 4 15. no. of figures 5
16. supplementary notes	
17. presented at (title, place, date) Proceedings of the Conference on Design, Automation and Test in Europe (DATE) 3001 Leuven, Belgium, 3/2013	
18. abstract The timing predictability of embedded systems with hard real-time requirements is fundamental for guaranteeing their safe usage. With the emergence of multicore platforms this task became very challenging. In this paper, a model- checking based approach will be described which allows us to guarantee timing bounds of multiple Synchronous Data Flow Graphs (SDFG) running on shared-bus multicore architectures. Our approach utilizes Timed Automata (TA) as a common semantic model to represent software components (SDF actors) and hardware components of the multicore platform. These TA are explored using the UPPAAL model-checker for providing the timing guarantees. Our approach shows a significant precision improvement compared with the worst-case bounds estimated based on maximal delay for every bus access. Furthermore, scalability is examined to demonstrate analysis feasibility for small parallel systems.	
19. keywords	
20. publisher European Design and Automation Association	21. price

Document Control Sheet

1. ISBN or ISSN 978-3642388521	2. type of document (e.g. report, publication) publication
3. title Exploiting Segregation in Bus-Based MPSoCs to Improve Scalability of Model-Checking-Based Performance Analysis for SDFAs	
4. author(s) (family name, first name(s)) Maher Fakih, Kim Grüttner, Martin Fränzle, Achim Rettberg	5. end of project 01.10.2014 6. publication date 06 / 2013 7. form of publication Inproceeding
8. performing organization(s) (name, address) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg Carl von Ossietzky University, Germany Ammerländer Heerstraße 114-118, 26129 Oldenburg	9. originator's report no. 10. reference no. 13N11480 11. no. of pages 13
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 16 14. no. of tables 1 15. no. of figures 2
16. supplementary notes	
17. presented at (title, place, date) 4th IFIP TC 10 International Embedded Systems Symposium, IESS 2013 Paderborn, Germany, 06 / 2013	
18. abstract The timing predictability of embedded systems with hard real-time requirements is fundamental for guaranteeing their safe usage. With the emergence of multicore platforms this task becomes even more challenging, because of shared processing, communication and memory resources. Model-checking techniques are capable of verifying the performance properties of applications running on these platforms. Unfortunately, these techniques are not scalable when analyzing systems with large number of tasks and processing units. In this paper, a model-checking based approach that allows to guarantee timing bounds of multiple Synchronous Data Flow Applications (SDFA) running on shared-bus multicore architectures will be extended for a TDMA hypervisor architecture. We will improve the the number of SDFAs being analyzable by our model-checking approach by exploiting the temporal and spatial segregation properties of the TDMA architecture and demonstrate how this method can be applied.	
19. keywords	
20. publisher Springer; Auflage: 2013 (28. Juni 2013)	21. price

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) publication

3. title
Multicore Performance analysis of a Multi-phase Electrical Motor Controller

4. author(s) (family name, first name(s))	5. end of project 01.10.2014
Maher Fakih, Kim Grüttner, Martin Fränzle, Achim Rettberg	6. publication date 02 / 2014
	7. form of publication Inproceeding
8. performing organization(s) (name, address) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg Carl von Ossietzky University, Germany Ammerländer Heerstraße 114-118, 26129 Oldenburg	9. originator's report no.
	10. reference no. 13N11480
	11. no. of pages 10
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 26
	14. no. of tables 0
	15. no. of figures 8

16. supplementary notes

17. presented at (title, place, date)
International Conference on Embedded Real Time Software and Systems 2014 (ERTS²)
Toulousse, France 02 / 2014

18. abstract

The timing predictability of embedded systems with hard real-time requirements is fundamental for guaranteeing their safe usage. With the emergence of multicore platforms this task becomes even more challenging, because of shared processing, communication and memory resources. In this paper, a combination of simulative method with a performance analysis based on model-checking is proposed. The simulative approach is used for functional validation of the Synchronous Data Flow Application (SDFA) implementation and its mapping on the targeted hardware platform. In our proposed methodology, we are using a binary-compatible and cycle-accurate virtual platform representation to simulate and map all relevant architectural properties to our analytical performance model. In combination, the model-checking based method allows to guarantee timing bounds of multiple Synchronous Data Flow Application (SDFA) implementations. This approach utilizes Timed Automata (TA) as a common semantic model to represent WCET of software components (SDF actors) and access protocols including timing of shared buses, shared DMAs, private local and shared memories of the multicore platform. The resulting network of TA is analyzed using the UPPAAL model-checker for providing safe timing bounds of the implementation. We demonstrate our approach using a multi-phase electric motor control algorithm (modeled as SDFA) mapped to Infineon's TriCore-based Aurix multicore hardware platform.

19. keywords

20. publisher Proceedings of ERTS² 2014	21. price

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) publication
3. title Hardware-Based Real-Time Simulation on the Raspberry Pi	
4. author(s) (family name, first name(s)) Walter, Jörg Fakih, Maher Grüttner, Kim	5. end of project 01.10.2014
	6. publication date 01 / 2014
	7. form of publication Inproceeding
8. performing organization(s) (name, address) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg	9. originator's report no.
	10. reference no. 13N11480
	11. no. of pages 12
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 22
	14. no. of tables 2
	15. no. of figures 4
16. supplementary notes	
17. presented at (title, place, date) 2nd Workshop on High-performance and Real-time Embedded Systems (HiRES 2014) Vienna, Austria, January 20, 2014	
18. abstract Hardware prototypes are commonly used during embedded control unit design. Existing commercial tools offer an integrated workflow from mathematical models down to hardware simulation. Researchers also build low-cost simulation platforms out of commodity equipment. We present a platform that is an order of magnitude cheaper than existing systems but still easy to integrate into present workflows: Within an existing model-driven design methodology, we perform real-time hardware simulation using the Raspberry Pi single-board computer to simulate an electromechanical system with little development effort."	
19. keywords	
20. publisher Proceedings of HiRES 2014	21. price

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) Poster
3. title Model-Based Design and Virtual Integration of an Intelligent and Safe Electrical Powertrain	
4. author(s) (family name, first name(s)) Sven Rosinger, Maher Fakih Jörg Walter	5. end of project 01.10.2014
	6. publication date 03 / 2014
	7. form of publication Conference Contribution
8. performing organization(s) (name, address) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg	9. originator's report no.
	10. reference no. 13N11480
	11. no. of pages 1
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references
	14. no. of tables 1
	15. no. of figures 5
16. supplementary notes	
17. presented at (title, place, date) Conference on Design, Automation and Test in Europe DATE'14 -University Booth Dresden, Germany, 2014	
18. abstract	
19. keywords	
20. publisher	21. price

Document Control Sheet

1. ISBN or ISSN 1383-7621	2. type of document (e.g. report, publication) publication
3. title State-Based Real-Time Analysis of SDF Applications on MPSoCs with Shared Communication Resources	
4. author(s) (family name, first name(s)) Maher Fakih, Kim Grüttner, Martin Fränzle, Achim Rettberg	5. end of project 05/2015 6. publication date To appear 05/2015 7. form of publication Journal Article
8. performing organization(s) (name, address) OFFIS – Institut für Informatik - Escherweg 2 26121 Oldenburg Carl von Ossietzky University, Germany Ammerländer Heerstraße 114-118, 26129 Oldenburg	9. originator's report no. 10. reference no. 13N11480 11. no. of pages 28
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 42 14. no. of tables 3 15. no. of figures 23
16. supplementary notes	
17. presented at (title, place, date) Journal of Systems Architecture (JSA) 2015	
18. abstract The timing predictability of Multi-Processor System on Chip (MPSoC) platforms with hard real-time applications is much more challenging than that of traditional platforms due to their large number of shared processing, communication and memory resources. Yet, this is an indispensable challenge for guaranteeing their safe usage in safety critical domains (avionics, automotive). In this article, a real-time analysis based on model-checking is proposed. The model-checking based method allows guaranteeing timing bounds of multiple Synchronous Data Flow Application (SDFA) implementations. This approach utilizes Timed Automata (TA) as a common semantic model to represent WCET of software components (SDF actors) and shared communication resource access protocols for buses, DMA, private local and shared memories of the MPSoC. The resulting network of TA is analyzed using the UPPAAL model-checker for providing safe timing bounds of the implementation. Furthermore, we will show the extension of our previous system model enabling single-beat inter-processor communication style beside the burst-transfer style and provide the implementation of the complete set of TA templates capturing the considered system model. We demonstrate our approach using a multi-phase electric motor control algorithm (modeled as SDFA) mapped to Infineon's TriCore-based Aurix multicore hardware platform with both the burst and single-beat inter-processor communication styles. Our approach shows a significant precision improvement (up to a percentage improvement of 300%) compared with the worst-case bound calculation based on a pessimistic analytical upper-bound delays for every shared resource access. In addition, scalability is examined to demonstrate analysis feasibility for small parallel systems, up to 40 actors mapped to 4-tiles and up to 96 actors on a 2-tiles platforms.	
19. keywords	
20. publisher Journal of Systems Architecture	21. price