NEWS

SafeTRANS
SAFETY IN TRANSPORTATION SYSTEMS

Cyber Physical Systems – Schlüssel für den Ausbau industrieller Kernkompetenzen

In ihrem aktuellen Jahresgutachten sieht die Expertenkommission *Forschung und Innovation* Deutschland in einem „Zangengriff zwischen Aufstiegsländern und klassischen Spitzentechnologieproduzenten". Deutschlands Stärken lägen in der Produktion von Hochtechnologieprodukten - z.B. im Automobilbereich und Maschinenbau - nicht jedoch in Spitzentechnologiesektoren wie der Informationstechnik (IT).

Diese Einschätzung der Experten ist nicht ganz neu. Das Beispiel eingebetteter Systeme zeigt jedoch, wie Hoch- und Spitzentechnologie in Deutschland integriert und produziert werden kann. Denn die gute Position der deutschen Industrie belegt, dass diese sehr wohl in der Lage ist, IT in Form vernetzter Bordcomputer in ihre Produkte zu integrieren. Im Automobilbau wird mittlerweile der größte Teil der Wertschöpfung durch eingebettete Computertechnik erzielt. Für die Entwicklung dieser Systeme ist ein hoher Aufwand erforderlich, der in erster Linie durch die Softwareentwicklung und die Vernetzung der Systeme bestimmt wird.
Der radikale technische Wandel bei eingebetteten Systemen führt zu gravierenden Konsequenzen: In naher Zukunft werden wir per Internet-Technik umfassend vernetzte eingebettete Systeme sehen, sogenannte *Cyber Physical Systems*, die als Bausteine in Alltagsgegenständen die reale und digitale Welt miteinander verknüpfen.

Die Bedeutung der IT für die Produktion von Hochtechnologiegütern wird mit Cyber Physical Systems (CPS) nochmals erheblich zunehmen. Zu den Kernkompetenzen der deutschen Industrie zählt die Entwicklung und Beherrschung komplexer Prozesse in Produktion und Distribution. Dies lässt sich ausbauen bei der Entwicklung von eingebetteten Systemen zu komplexen CPS.
Um Deutschlands Stärken zu erhalten und zu erweitern, hat die Bundesregierung eine Forschungsroadmap zu CPS entwickeln lassen - agendaCPS - und fördert die Umsetzung in allen wichtigen Branchen. So werden Werkzeuge für die Praxis beispielsweise im Projekt *SPES XTCore* entwickelt und anwendungsnahe Prozesse für die industrielle Produktion und Logistik im Projekt *Industrie 4.0* im Rahmen der Hightech-Strategie umgesetzt. CPS ermöglichen neue Produktions- und Geschäftsmodelle mit erheblichen Optimierungspotenzialen bei größerer Individualisierung von Produkten und dies zu Preisen wie in einer Massenproduktion. Erste Bausteine sind bereits entwickelt und in der Praxiserprobung. Der entscheidende nächste Schritt ist die Verknüpfung dieser Bausteine zu umfassenden Systemverbünden und Geschäftsprozessen.
Die Bundesregierung unterstützt diese Entwicklungen, um die damit verbundenen Chancen zu nutzen.

Dr. Georg Schütte,
Staatssekretär im Bundesministerium für Bildung und Forschung

Inhalt

Aktuelle Meldungen 2
Termine 5
SafeTRANS Gespräche: Karsten Lemmer, DLR 6
SafeTRANS Mitglieder stellen sich vor: ICS AG 8
ITEA 3 - Neueste Informationen 10
Fachartikel: Critical Systems Engineering 12
ARAMiS - Erste Ergebnisse 14
SPES 2020 - Entwicklung einer neuen Modellierungsmethodik 15
SafeTRANS Mitglieder 16

Aktuelle Meldungen

Neues aus dem Forschungs- und Wirtschaftsumfeld

TTTech verstärkt SafeTRANS im Bereich modulare Sicherheitsplattformen

Seit Mai 2012 ist das österreichische Unternehmen TTTech Computertechnik AG Mitglied bei SafeTRANS. Die Kompetenzen des mittelständischen Unternehmens liegen bei der Verbesserung der Sicherheit und Zuverlässigkeit von vernetzten elektronischen Systemen in der Industrie und Transportbranche. TTTech ist führender Lösungsanbieter für zuverlässige Netzwerklösungen basierend auf zeitgesteuerter Technologie und modularen Sicherheitsplattformen. Das Produktportfolio ist gemäß den Anforderungen von IEC 61508, ISO 26262, EN 13849, DO-254 und DO-178B zertifizierbar.
TTTech Lösungen kommen z.B. im Airbus A380, dem Boeing 787 Dreamliner und den neuen Audi-Modellen A8, A7 und A6 zum Einsatz. Im Jahr 2012 investiert das Unternehmen 20 Mio. Euro in FuE. Diese Aktivitäten werden u.a. durch SafeTRANS weiter unterstützt.
TTTech wurde 1998 als Spin-Off der TU Wien gegründet und ist international tätig. Neben dem Hauptsitz in Wien ist TTTech in Deutschland, Italien, der Tschechischen Republik, Rumänien, den Vereinigten Staaten, Japan, Korea und China vertreten.
www.tttech.com

Ensuring Reliable Networks TTTech

Karlheinz Topp vertritt Bosch in SafeTRANS und im EICOSE Steering Board

Karlheinz Topp übernahm im Mai 2012 die Nachfolge als Vertreter der Robert Bosch GmbH in SafeTRANS sowie als Vertreter von SafeTRANS im EICOSE Steering Board von Wolfgang Klingenberg, der in den Ruhestand gegangen ist. In beiden Funktionen ist Karlheinz Topp Ansprechpartner für FuE-Projekte im Bereich Prozesse und Methoden für Embedded Systems der Robert Bosch GmbH: bei SafeTRANS im nationalen Kontext und bei EICOSE für europäische Themen.


Karlheinz Topp

Karlheinz Topp ist bei der Robert Bosch GmbH im Zentralbereich Forschung und Vorausentwicklung als Koordinator für öffentliche Projekte zuständig. Die Robert Bosch GmbH ist SafeTRANS-Mitglied seit dessen Gründung im Jahr 2006.
Informationen zur Organisationsstruktur von SafeTRANS und EICOSE finden Sie hier:
http://safetrans-de.org/de_structure.php
http://eicose.eu/index.php?id=structure

EICOSE European Institute for Complex Safety Critical Systems Engineering

H. Portier und W. Damm leiten ARTEMIS-IA Working Group Tool Platforms

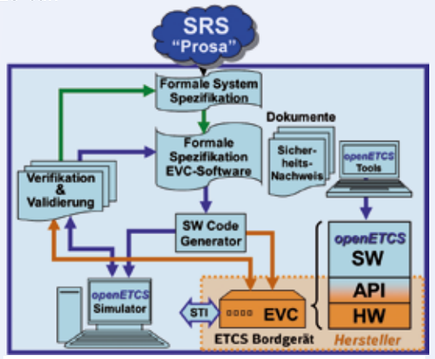
Ab Mai 2012 wird die ARTEMIS-IA Working Group *Tool Platforms* von Hervé Portier (Airbus Frankreich) und Prof. Dr. Werner Damm (OFFIS, SafeTRANS) geleitet. Durch die Ernennung der beiden neuen Chairmen wird eine konstruktive Weiterführung der begonnenen Aktivitäten hinsichtlich Erstellung, Koordinierung und Etablierung von Tool Plattforms sichergestellt. Diese Werkzeug-Plattformen bauen auf Ergebnissen von europäischen Forschungsprojekten, u.a. im Rahmen des ARTEMIS- und ITEA-Programms auf, und machen z.B. Spezifikationen für Prozesse und Methoden zur Entwicklung von eingebetteten Systemen verfügbar. So wird die Produktivität und Nachhaltigkeit von FuE-Projekten durch den Austausch von Forschungsergebnissen und der domänenübergreifenden Wiederverwendung von Technologien gefördert.
Hervé Portier und Werner Damm sind gleichzeit auch im Steering Board von EICOSE, dem European Insitute for Complex Safety Critical Systems Engineering, vertreten. Weitere Informationen zu den ARTEMIS Tool Platforms finden Sie unter folgendem Link:
www.artemis-ia.eu/tool_platforms


Werner Damm


Hervé Portier

OpenETCS soll Zugsicherung interoperabel, sicher und bezahlbar machen

ETCS (European Train Control System) soll in Europa rund 30 teilweise veraltete Signal- und Zugsicherungssysteme ablösen und mit mehr „Intelligenz“ auf den Fahrzeugen die Streckenausrüstung vereinfachen. Man verspricht sich von ETCS die Überwindung nationaler Schranken, mehr Wettbewerb und insgesamt geringere Kosten für das System Bahn. Mehr als 20 Jahre nach Projektbeginn und nach rund 10 Jahren Produktentwicklung gibt es in Europa zwar rund 4.000 km Strecke mit ETCS-Ausrüstung, aber noch kein einziges ETCS-Fahrzeuggerät, das auf allen Strecken zugelassen werden konnte, obwohl eine detaillierte technische Spezifikation (SRS) - was einzigartig ist - öffentlich zugänglich ist. Die Gründe dafür sind vielfältig: Hohe Komplexität eines multinationalen Systems, aber keine anerkannte Referenzimplementation; eine interpretierbare (Prosa-)Spezifikation, kombiniert mit Human Factors und nationale Besonderheiten führen zwangsläufig zu Abweichungen.
Mit Hilfe des Projekts *openETCS* soll sich dies ändern. Dabei wird ein neues Konzept namens *open Proofs* eingesetzt. Open Proofs ist als Erweiterung von Free/Libre Open Source Software (FLOSS) für kritische Systeme zu verstehen. Es werden nicht nur die Software der Endprodukte (hier ETCS-Bordgerät) als FLOSS lizenziert, sondern auch alle Werkzeuge und Dokumente, die für Spezifikation, Entwicklung, Betrieb und Wartung erforderlich sind, einschließlich der formalen (Sicherheits-)Nachweise, kurz „Proofs“ genannt. Die FLOSS-Lizensierung aller Komponenten hat einen stark standardisierenden Effekt und unterstützt vorwettbewerbliche Kooperation (Open Source Konsortium). Kombiniert mit weltweiten Experten-Peer-Reviews („viele Augen-Prinzip“) erwartet man höhere Qualität, im Sinne von mehr Zuverlässigkeit, bei gleichzeitig sinkenden Kosten.



Das Prinzip: Aus formaler Spezifikation mit FLOSS-Werkzeugkette generierte und formal verifizierbare SW erfordert ein Standard-API (Application Programming Interface), um auf EVCs (European Vital Computer) unterschiedlicher Hersteller eingesetzt werden zu können.

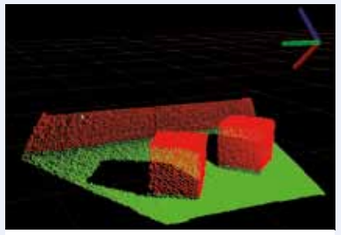
Dieses Forschungs- und Entwicklungsprojekt mit zwölf Partnerorganisationen aus Deutschland und weiteren 26 europäischen Partnern wird im ITEA2-Programm vom BMBF mit 4,5 Mio. Euro über einen Zeitraum von drei Jahren gefördert. Das Projekt startet im Juli 2012 und wird von der Deutschen Bahn AG geleitet.
www.openetcs.info
Ansprechpartner:
Dr. Klaus-Rüdiger Hase:
klaus-ruediger.hase@deutschebahn.com

Bundesministerium für Bildung und Forschung
ITEA 2

Sicherer Kegelscanner verhindert Kollisionen

Ein intelligenter Scanner schützt autonom fahrende Industriefahrzeuge vor Kollisionen, indem er diese vorhersieht: Im kürzlich abgeschlossenen Projekt IGEL (Sicherer Kegelscanner) entwickelten Wissenschaftler am DFKI-Forschungsbereich “Cyber-Physical Systems” (CPS) unter der Leitung von Prof. Dr. Rolf Drechsler die Software für einen Laserscanner oder vergleichbaren Sensor, der anstelle der üblichen zweidimensionalen eine kegelförmige Fläche abtastet.
Der Sensor blickt dabei von oben auf den Boden und kann auf diese Weise sowohl Hindernisse beliebiger Höhe über dem Boden als auch Unebenheiten im Boden (Löcher, Gräben) erfassen. Hierzu wurde eine Software entwickelt, die aus dreidimensionalen Messwerten (einer sogenannten „Punktwolke“) eine Bodenebene berechnet, und auf dieser sowohl positive, d.h. aus ihr herausragende, als auch negative Hindernisse, wie Löcher und Abgründe, ab einer konfigurierbaren Mindestgröße erkennt. Diese führen zu einem Nothalt.

Einzelne Messfehler, beispielsweise durch Luftverunreinigungen (Staub, Wassertropfen), werden toleriert, sodass nicht jede Fehlmessung einen Nothalt nach sich zieht; dies ist in Industrieumgebungen ein wichtiges Verfügbarkeitsmerkmal.



Screenshot des Projekt-Demonstrators: Mit einer Kinect als Sensor werden der Boden (grün) und Hindernisse (rot) sicher erkannt.

Das Konzept und die Gefährdungsanalyse für beide Algorithmen wurden vom TÜV Nord begutachtet und „sind geeignet, eine Hinderniserkennung für autonome Fahrzeuge zur Risikominimierung gemäß 2006/42/EG Anhang I zu realisieren“, d.h. sie sind als Sicherheitseinrichtung nach der Maschinenrichtlinie zulässig. Die Algorithmen wurden prototypisch implementiert und sind als ROS-Pakete verfügbar.

Die entwickelten Konzepte lassen sich sowohl zur Absicherung eines autonomen Fahrzeugs verwenden als auch als Assistenzeinrichtung eines gesteuerten Fahrzeugs, beispielsweise um die Rückwärtsfahrt eines Staplers abzusichern. Im Vergleich zu konventionellen Lösungen mit horizontal detektierenden Laserscannern werden Kollisionsschutz und Fahrzeugsicherung signifikant verbessert.

Das Projekt IGEL wurde vom DFKI in Zusammenarbeit mit der Firma Götting KG durchgeführt und vom BMBF im Rahmen des Programmes „KMU-innovativ“ gefördert.

www.dfki.de/cps/igel

DFKI-Kontakt:
Prof. Dr. Christoph Lüth
Christoph.Lueth@dfki.de

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

Workshop zu Methoden, Prozessen und Tools im Automobilbereich

Um Wissen und Informationen rund um Forschung für Methoden, Prozesse und Tools im Bereich Automobilbau zu unterstützen, widmet sich ein gemeinsamer Workshop der öffentlich geförderten Projekte AMALTHEA, TIMMO-2-USE, SAFE (Projekte des ITEA2-Programms) und MAENAD (FP7-Programm) dem Thema *Challenges, methodologies, representations and tooling for automotive embedded systems*.

Der Workshop findet am 24. und 25. September 2012 in Berlin statt. Er richtet sich an Forscher und Entwickler aus Industrie und Wissenschaft, die an den Projekten beteiligt sind sowie an Personen mit generellem Interessen an diesem Themenfeld. Eine Anmeldung bei den Projektkoordinatoren ist erforderlich. Dort können auch weitere Informationen erfragt werden.

Projekt	Koordinator
AMALTHEA	K. Topp: karlheinz.topp@de.bosch.com
MEANAND	H. Lönn: henrik.lonn@volvo.com
SAFE	S. Voget: stefan.voget@continental-corporation.com
TIMMO-2-USE	D. Karlsson: daniel.b.karlsson@volvo.com

Automatisch synthetisierte Diagnoseeinheiten

Die BTC Embedded System AG untersucht zur Zeit, zusammen mit namhaften Automobilherstellern, die Möglichkeit aus formalen Anforderungsspezifikationen mittels automatisch generierter C-Code-Observer („watch dogs“) On-Board-Diagnoseeinheiten zu synthetisieren. Diese Diagnoseeinheiten laufen dann während des Tests parallel zu den eigentlichen Fahrzeugfunktionen auf dem Steuergerät im Fahrzeug mit. Bei fehlerhaften funktionalen Verhalten der Fahrzeugfunktionen sind die Diagnoseeinheiten in der Lage spezifische Anforderungsverletzungen der Fahrzeugfunktionen zu lokalisieren. Durch die bidirektionale Verlinkung sämtlicher Artefakte im modellbasierten Entwicklungsprozess, bis hin zur ursprünglichen Anforderung, lässt sich die Ursache einer möglichen Fehlfunktion erheblich leichter und automatisierter lokalisieren, als dies mit gegenwärtigen konventionellen Debug-Methoden möglich ist. Es wird zusätzlich auch darüber nachgedacht, die Diagnoseeinheiten für eine automatische Fehlerkorrektur im fahrenden Fahrzeug zum Einsatz zu bringen, um eine Überwachung zur Fahrzeit zu unterstützen. Die formalisierte Spezifikation der Anforderungen und das automatische Synthetisieren der Diagnoseeinheiten mittels C-Code-Observer werden hier mit BTC EmbeddedSpecifier Technologie durchgeführt, welche zum Teil im Rahmen des CESAR Projektes entwickelt wurde.

www.btc-es.de

BTC

Termine

Messen und Kongresse

10.-12.09.2012
61. Deutscher Luft- und Raumfahrtkongress 2012
Berlin
www.dlrk2012.dglr.de

11.-16.09.2012
ILA Air Show
Berlin
www.ila-berlin.de

30.-31.10.2012
ARTEMIS / ITEA-Co-Summit
Paris (Frankreich)
www.artemis-ia.eu
www.itea2.org

13.-16.11.2012
electronica
München
www.electronica.de

15.-16.11.2012
ITAFourm
Berlin
www.itaforum.info

Konferenzen, Tagungen und Seminare

11.-12.09.2012
30th European Annual Conference on Human Decision-Making and Manual Control
EAM 2012
Braunschweig
www.eam2012.net

12.-14.09.2012
HCI-Aero 2012
International Conference on Human-Computer Interaction in Aerospace
Brüssel (Belgien)
http://research.fit.edu/hci-aero/HCI-Aero2012/Home.html

16.-21.09.2012
Cyber-Physical Systems: Chancen, Risiken, Aussichten – Workshop auf der INFORMATIK 2012, der 42. Jahrestagung der Gesellschaft für Informatik
Braunschweig
www.informatik2012.de

17.-21.09.2012
ARTIST Summer School on Embedded Systems
Aix-les-Bains (Frankreich)
http://artist-summer-school.epfl.ch

20.-21.09.2012
ARTEMIS-Austria Conference - Future Embedded Systems Solving Societal Challenges
Wien (Österreich)
www.artemis-austria.net

24.-25.09.2012
Open Workshop on challenges in automotive specific methodologies, representations and tooling
Berlin
Kontakt: siehe Aktuelle Meldungen, Seite 4

25.-28.09.2012
31st International Conference on Computer Safety, Reliability and Security
Magdeburg
www.ovgu.de/safecomp

26.-27.09.2012
6th Symtavision NewsConference
Braunschweig
http://www.symtavision.com/newsconference2012.html

26.-28.09.2012
20 years of Verimag
Grenoble (Frankreich)
www-verimag.imag.fr/20-years-of-Verimag.html?lang=en

27.-28.09.2012
ATAMI 2012 – Advances in Testing: Academia Meets Industry
Berlin
www.first.fraunhofer.de/home/aktuell/atami-2012/

07.-12.10.2012
Embedded Systems Week
Tampere (Finland)
www.esweek.org

17.-19.10.2012
QA&TEST 2012
Bilbao (Spanien)
www.qatest.org/en

08.-09.11.2012
20th International Conference on Real-Time and Network Systems
Pont à Mousson (Frankreich)
http://rtns2012.loria.fr

03.-07.12.2012
Embedded Software Engineering Kongress
Sindelfingen
www.ese-kongress.de

12.-13. Dezember 2012
FORMS /FORMAT 2012 - 9th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems
Braunschweig
www.iva.ing.tu-bs.de

„Es gilt, das intelligente Mobilitätskonzept der Zukunft mitzugestalten.“

Das DLR verankert mit der *Anwendungsplattform Intelligente Mobilität* (AIM) Forschungs- und Entwicklungsaktivitäten im offenen Straßenraum. Das Land Niedersachsen, die Stadt Braunschweig und weitere Partner aus Industrie und Forschung arbeiten im Projekt AIM gemeinsam daran, die urbane Mobilität ganzheitlich zu erfassen. Und was kann es Spannenderes geben, als neue Technologien im Alltag zu testen? Prof. Dr.-Ing. Karsten Lemmer, Direktor des Instituts für Verkehrssystemtechnik im DLR, stellt erste Ergebnisse und zukünftige Mobilitätskonzepte vor.

Was sind aktuell wichtige Forschungsthemen im Bereich Embedded Systems (ES) für das DLR?
Karsten Lemmer: Wir sehen steigende Anforderungen im Bereich der Zuverlässigkeit und Hochverfügbarkeit von ES und den entsprechenden Applikationen. Vernetzte ES sind die Grundlage für verteilte Anwendungen, deren Bedarf in Zukunft steigen wird. Dadurch ergeben sich neue Herausforderungen in den Bereichen Entwurf und Test - und über die Lebenszyklen hinaus auch im Bereich der Virtualisierung.

Das stark praxisorientierte Projekt AIM startete 2011. Sind bereits erste Ergebnisse verfügbar?
Erste Prototypen und Dienste werden derzeit genutzt. Ein Beispiel ist das Projekt SimWorld. Hier werden Daten erhoben und ausgewertet mit dem Ziel, Simulationsmodelle und virtuelle Testumgebungen zu generieren sowie den Erstellungsprozess ein Stück weit zu automatisieren. Die Simulatoren werden u.a. beim Testen von Fahrerassistenzsystemen (FAS) eingesetzt.
In einem anderen Projekt untersuchen wir komplexe Kreuzungen und analysieren das Verhalten von Verkehrsteilnehmern in Beinah-Unfallsituationen. Eine Studie mit Fahrzeugherstellern, die Anforderungen an Forschungskreuzungen spezifiziert, konnte bereits erstellt werden.
Des Weiteren statten wir seit August 2011 Ampelanlagen in Braunschweig mit Funkanlagen aus. Über WLAN teilen die Ampeln den Versuchsfahrzeugen mit, wie lange sie noch grün oder rot bleiben. Mit diesen Werten ist das DLR-Versuchsfahrzeug FASCar dann in der Lage, dem Fahrer im Tacho eine Geschwindigkeitsempfehlung anzuzeigen. So kann der Fahrer ungebremst und flüssig durch den Braunschweiger Stadtverkehr fahren - vorausgesetzt er hält sich an die Geschwindigkeitsempfehlung.


FAS-Anzeige im Tachometer für eine „grüne Welle“.

Für umfassende Mobilitätskonzepte ist es nötig, den Verkehr in einem ersten Schritt zu erfassen (Monitoring) und im Weiteren zu beeinflussen. Welche Formen des Verkehrs-Monitorings gibt es?
Man unterscheidet die Erfassung von stationären und dynamischen Daten. Stationäre Daten werden z.B. über Sensoren an Ampeln als Schleifendaten erfasst.
Zur Erfassung von dynamischer Information nutzt das DLR sogenannte Floating Cars. Dabei werden mithilfe von Fahrzeugen, die mit bestimmten Sensoren ausgestattet sind, z.B. Taxen, kontinuierlich Daten über den Verkehrsfluss erfasst. Der Vorteil liegt darin, dass mit einigen Zusatzinformationen Reisezeiten ermittelt werden können. Für Endnutzer ist es wichtig zu wissen, wie lange man von Ort A zu Ort B benötigt und nicht, wieviele Autos an einer bestimmten Kreuzung vorbeifahren. Neben den Floating Cars nutzen wir für die Erfassung von dynamischen Daten Nomadic Devices, die mit Bluetooth-Technologie arbeiten.
Ziel unserer Forschung ist nicht die Erstellung von Nutzerprofilen einzelner Individuen, sondern Bewegtdaten von Objekten im Straßenverkehr zu ermitteln. So können wir unterschiedliche Verkehrsteilnehmer in detailreiche Modelle integrieren, die aus stationären und dynamischen Daten generiert werden. Diese Modelle sind sehr wichtig für unsere Forschungsarbeit, denn sie dienen der Unfallforschung und sind ein wichtiger Faktor für eine zielgerichtete Entwicklung von FAS bezüglich individueller Bedürfnisse im Gesamtverkehrskontext. Zudem erlauben sie uns, Prognosen zur Verkehrsentwicklung mit unterschiedlichen Zeithorizonten anzustellen.

Welche Möglichkeiten zur Finanzierung von neuen Lösungen im Verkehrsmanagement, wie sie beispielsweise in AIM erforscht werden, sehen Sie?
Ich kann mir unterschiedliche Finanzierungsmodelle aus öffentlichen und privaten Investitionen vorstellen. Für Kommunen kann es sich lohnen, in neue Verkehrssysteme zu investieren, um z.B. das Vorrecht von Rettungsfahrzeugen sicherzustellen. Dadurch kann die Effizienz gesteigert werden und weniger Feuerwachen wären notwendig. Ein Anreiz könnte auch die Reduzierung von Feinstaub und Emissionen sein. Im Bereich von FAS ist denkbar, dass Automobilhersteller sich an der Finanzierung beteiligen, da ein direkter Mehrwert über mehr Komfort und eine verbesserte Verkehrsführung erreicht werden kann.
Grundsätzlich können im Gesamtkonzept der vernetzten Anwendungen die meisten Vorteile erzielt werden: Mit Daten aus dem Verkehrsfluss (Floating Cars), stationären Daten (Ampeln mit Funkausstattung) sowie mit der darauf basierend angepassten Verkehrsführung kann die Mobilität effizienter, effektiver und angenehmer gestaltet werden.

Interoperabilität von Entwicklungs-Software ist wichtig, um Prozesse zu beschleunigen. Wie schätzen Sie die Situation in den Transportbereichen Automotive, Bahn und Luftfahrt ein?
Ich sehe ein verstärktes Zusammenwachsen von Werkzeugen für sicherheitskritische Anwendungen. Der Bedarf an hoch entwickelten Entwurfs-, Implementierungs- und Testwerkzeugen sowie deren Interoperabilität ist bereits vorhanden und auch zwingend erforderlich, um die Komplexität von zukünftigen Systemapplikationen beherrschen zu können.
Langfristig können mit hoher Interoperabilität auch verstärkt wirtschaftliche Möglichkeiten erschlossen werden, denn der Markt kann mit einer breiten Anwendbarkeit der Werkzeuge wachsen. Es ist eine strategische Frage für Unternehmen, diesen Markt zu schaffen und zu vergrößern. Die Erfahrung aus anderen Branchen, z.B. der Produktionsautomatisierung, zeigt, dass Protektion nur eine gewisse Zeit aufrechterhalten werden kann und Durchgängigkeit über offene Strukturen der Schlüssel für die Zukunft ist.

In 2011 feierte das Institut für Verkehrssystemtechnik zehnjährigen Geburtstag. Was hat man bisher erreicht und wo möchte man in den nächsten zehn Jahren hin?
Wir haben im Bereich der menschzentrierten Entwicklung von Assistenzsystemen und Automatisierung bei verschiedenen Verkehrsträgern, der Erstellung von Gesamtkonzepten sowie bei der Entwicklung von Sicherheitsarchitekturen erhebliche Beiträge geleistet. Unsere breite Datenbasis wird nicht nur in der Theorie eingesetzt, sondern auch in der prototypischen Anwendung.
Zukünftig glaube ich, dass die Entwicklung von formalen und modellbasierten Methoden noch stärker an Bedeutung gewinnen wird. Ein weiteres Feld betrifft die Nutzbarmachung von Daten, denn mit dem enorm wachsenden Datenvolumen muss auch eine Aufbereitung und Auswertung einhergehen.
Mit unserem Institut ist es uns gelungen, den Bereich der neutralen, interdisziplinären Forschung in der Mobilität zu manifestieren. Wir merken bei der Zusammenarbeit mit Partnern, dass die fachliche und wirtschaftliche Kooperation einen höheren Stellenwert als die Interessenvertretung hat. Diesen Vorteil der Neutralität sehe ich auch bei SafeTRANS, wo FuE-Akteure im Bereich ES domänenübergreifend ihre Aktivitäten bündeln. Denn es gilt, das intelligente Mobilitätssystem der Zukunft mitzugestalten.

Vielen Dank für das Gespräch!

Karsten Lemmer

Professor Dr. Karsten Lemmer ist seit 2001 Direktor des Instituts für Verkehrssystemtechnik im Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR) sowie Universitätsprofessor an der Technischen Universität Braunschweig.
Nach seinem Studium der Elektrotechnik von 1984 bis 1989 und der Promotion zum Thema „Diagnose diskret modellierter Systeme mit Petrinetzen“ an der TU Braunschweig, schlossen sich Tätigkeiten im Rahmen von Consultingprojekten im Bereich der Automatisierungs- und Automobiltechnik an. Anschließend war er bei der Siemens AG tätig.

Für sichere, vernetzte Systeme weltweit im Einsatz: Die Ingenieure der ICS AG

Was wäre das für eine Welt, in der Züge sich gegenseitige melden, dass die voraus liegende Strecke frei ist, Flugzeuge sich gegenseitig warnen, indem sie sich selbstständig ihre Position mitteilen und Autos an roten Ampel automatisch die Geschwindigkeit reduzieren? Ein Stück sicherer. Utopie? Mit Sicherheit nicht. Diese Dinge sind heute schon möglich, sie machen unseren Alltag sicher, ohne dass es die Reisenden merken oder der Komfort darunter leidet.

Wie ist das möglich? Unter anderem mit modernster Hightech, wie beispielsweise leistungsfähigen Netzwerken und rasanter Datenfunktechnik. Mit Ingenieuren, die um geltende Normen wissen sowie diese mit und weiterentwickeln. Mit Profis im Quality-Bereich, die Software und Systeme nicht nur programmieren, sondern definieren, prüfen und bis zur Zulassung begleiten. Mit Menschen, die sich für ihre Aufgaben begeistern und Ideen umsetzen.

Diese Spezialisten finden sich unter dem Dach der ICS AG. Die ICS bedient mit ihren Business Units die Branchen Automotive, Bahntechnik, Luft- und Raumfahrt, Verteidigungstechnik sowie den Maschinen- und Anlagenbau. Das branchenübergreifende Leistungsspektrum umfasst die Software- und Systementwicklung, die Technologie- und Prozessberatung bis zum Projekt- und Qualitätsmanagement. Die ICS ist Partner der weltweit führenden Unternehmen der jeweiligen Branchen für den kompletten Produktlebenszyklus der eingesetzten, hochkomplexen Systeme.

Schwerpunkt: Safety-, Mission- und Business-Critical Systems

Das Unternehmen ist branchenübergreifend tätig als Spezialist für Safety-, Mission- und Business-Critical Systems und liefert sowohl komplette maßgeschneiderte Software- und Engineering-Lösungen, als auch Support durch versierte Fachexperten von der Konzeption bis zur Zulassung dieser Systeme nach den jeweils relevanten Normen: EC 61508, ISO 26262, RTCA DO-178B, EN 50126, EN 50128 und EN 50129.

Das branchenspezifische Wissen wird in den vier Business Units *Transportation, Industrial Solutions, Automotive und Advanced Technologies* entwickelt und vertieft. In den an Prozessmodellen und Normen ausgerichteten *Competence Centern*, z.B. für Systems Engineering, Software Development, Verification & Test, Validation, RAMS, Assessment und Quality Assurance, wird Unit-übergreifend gearbeitet und es werden mögliche Synergieeffekte optimal genutzt.

Die **Business Unit Transportation** entwickelt sicherheitsrelevante Software und Systeme für die führenden Bahnsystemlieferanten rund um den Globus. Die ICS hat sich als unabhängiger Entwicklungsdienstleister in der Bahntechnik etabliert und das Dienstleistungsspektrum sowie Applikations-Know-how konsequent ausgebaut. Für die Leit- und Sicherungstechnik (ESTW, ETCS), als auch für die elektronischen Komponenten und Leitsysteme von Schienenfahrzeugen (TCMS) bietet die ICS kompetente und umfangreiche Engineering-Dienstleistungen an.

Cid Kiefer, Vorstand der ICS AG, mit seinem Team in Stuttgart.

Die Spezialisten der **Business Unit Industrial Solutions** unterstützen die Kunden im Bereich der Fertigungslogistik (Supply-Chain-Management), Infrastruktur, dem Qualitäts-Management sowie beim Betrieb von ERP-Systemen mit Fokus SAP und Logistik. Dies umfasst Prozessanalyse, Projektmanagement, Anforderungsdefinition, Technologieberatung, Implementierung und Integration. Für die Dienstleistungen kommen selbst entwickelte Frameworks zur Implementierung sowie Modelle zur Generierung (MDD, MDA) zum Einsatz.

Für Analyse und Design werden bewährte und akzeptierte Standards, wie z. B. UML 2.0, genutzt.

In der **Business Unit Automotive** werden zukunftsweisende embedded Software-Lösungen für Steuergeräte, Kommunikationsplattformen und Multimediaarchitekturen im Fahrzeug entwickelt. Basis sind etablierte BUS-Systeme (LIN, CAN, MOST®, FlexRay™) und Software-Architekturen nach AUTOSAR®. Das Leistungsspektrum umfasst Requirements Engineering, Systems Engineering, Software Engineering bis hin zur Realisierung von sicherheitskritischen Applikationen gemäß ISO 26262. Die ICS AG ist deutschlandweit und international im Einsatz für verschiedenen Hersteller und Zulieferer in den Bereichen Telematik und Infotainment, wo Navigationskernels getestet und konzeptioniert und HMI-Schnittstellen entwickelt werden. Dazu kommt Car-2-X Communication, bei der das Fahrzeug mittels Datenfunk mit Einrichtungen der Infrastruktur kommuniziert, sowie die Entwicklung von Demonstratoren für E-Mobility und der Weiterentwicklung der Fahrzeugvernetzung. Weitere Schwerpunkte sind die Anwendungsbereiche Fahrwerk und Antriebsstrang inklusive X-by-Wire und das Batteriemanagement.

Die **Business Unit Advanced Technologies** fast das Experten-Team aus dem Bereich Luft- und Raumfahrt und ein eigenes Methodenteam zusammen. Das Methodenteam kümmert sich unternehmensweit um die Optimierung und Standardisierung aller relevanten Methoden, Prozesse und Tools. Wichtige Arbeitsprinzipien sind die Auswertung von Lessons Learned mit der Identifikation und Sammlung von Best Practices sowie Pilotierung und Evaluierung neuer Methoden, Prozesse und Tools.

Das Aerospace & Defence-Team entwickelt Lösungen und Konzepte für sicherheitsgerichtete Systeme. Das Leistungsspektrum reicht dabei vom Requirements Engineering über Safety Management und modellbasierte Softwareentwicklung bis zur Verifikation und Validation. Die Anwendungen betreffen sowohl On-Board Geräte (bis Level A / SIL 4) gemäß DO-178B beziehungsweise DIN EN 61508, als auch Bodenstationen und Missionsplanungstools.

Nachhaltigkeit durch Zusammenarbeit

Ihr nachhaltiges Engagement bringt die ICS als Mitglied in maßgebenden Organisationen und Verbänden ein. So ist sie beispielsweise Mitglied des VDB e.V. (Verband der Bahnindustrie in Deutschland), der Gesellschaft für Informatik sowie seit 2010 in SafeTRANS.

www.ics-ag.de

SHORTCUTS: ICS AG

Unternehmen:	Informatik Consulting Systems AG
Unternehmenssitz:	Stuttgart
Gründung:	1966
Umsatz:	11,2 Mio. Euro
Mitarbeiter:	150

Fragen an Cid Kiefer, Vorstand ICS AG:

Wo sehen Sie im Bereich der Software- und Systementwicklung die größte Herausforderung der Zukunft?

Eine sehr große Herausforderung liegt in der Abwägung von generischen und individuellen Anteilen in der Software (SW). Der Kunde wünscht sich häufig speziell zugeschnittene Lösungen, gleichzeitig müssen die Systeme gut wartbar und Release-fähig bleiben. Dafür ist allerdings weniger Individualisierung und mehr Generalisierung nötig. Mithilfe der Parametrisierung eines generischen Ansatzes an spezielle Anforderungen kann dies gelingen.

Sehen Sie bezüglich Generalisierung bzw. Standardisierung Unterschiede in den Branchen?

Die Bereiche Aerospace, Transportation und Defence sind klassische Oligopole, mit relativ geschlossenem Markt. Standardisierung ist hier nicht so stark zu spüren. Im Automotive-Bereich dagegen sind die Standardisierungsbestrebungen höher, weil die Produktlebenszyklen viel kürzer sind und der Aufwand bei Systemwechseln damit sehr viel größer ist. Hier wird die Standardisierung bis zu einem gewissen Grad von den OEMs unterstützt. Andererseits stehen die Automobilhersteller vor der oben genannten Herausforderung der Differenzierung, die stark an die Systemlieferanten geknüpft ist. Allerdings haben die OEMs in der Vergangenheit die Systemintegration unterschätzt. Die SW ist zunehmend ein Abgrenzungsmerkmal und die Qualität wird immer wichtiger. Nur ein „Montage-OEM“ zu sein, der sich auf die Systeme der Lieferanten verlässt, reicht nicht aus. Die Komplexität der Gesamtarchitektur muss beachtet werden. Die Systemintegration und der Testaufwand sind dabei beachtlich - und in diesem Punkt sind sich alle Domänen ähnlich.

Was fasziniert Sie persönlich an Embedded Systems?

Das Zusammenspiel von HW und SW in diesen Regelkreis-basierten Systemen ist wahnsinnig spannend, vor allem hinsichtlich Antwortzeiten, Selbstüberwachung, Zuverlässigkeit, Sicherheit und Abdeckung der Anforderungen. Embedded Systems können menschliches Fehlverhalten ausgleichen, sind aber vom Menschen geschaffen und werden, trotz extremer Komplexität, (noch) vom Menschen kontrolliert.

ITEA 3 will europäische IKT-Forschung dynamischer machen

Schnellere Prozesse, mehr Kooperationen und digitale Roadmap werden wichtige Bestandteile von ITEA 3 ab 2014 sein.

EUREKA, die europäische Netzwerkinitiative zur Förderung anwendungsorientierter Forschung und Entwicklung in internationalen Kooperationsprojekten, hat offiziell ITEA 3 auf einer Tagung im Juni in Budapest beschlossen. ITEA 3 wird ab 2014 einen hoch dynamischen und flexiblen Ansatz zur Unterstützung von internationalen FuE-Projekten etablieren.

ITEA 3 - Was bleibt? Was ändert sich?

ITEA ist eine von der Industrie getriebene Initiative, die mit einem markt- und bottom-up-orientierten Ansatz vorwettbewerbliche, länderübergreifende Forschungsprojekte unterstützt. Inhaltlich konzentriert sich ITEA auf Fragestellungen im Bereich der Software-intensiven Systeme und Dienstleistungen, wozu beispielsweise intelligente Infrastrukturen, serienmäßige und individuelle Produkte und Dienstleistungen, innovatives Engineering sowie Systemsicherheit gehören. Dieses breite Themenspektrum wird auch weiterhin in der zweiten Verlängerung von ITEA bestehen bleiben.

Das große strategische Ziel von ITEA 3 ist eine hoch flexible Unterstützung von FuE-Projekten, um auf die sich wandelnden Bedürfnisse und Bedingungen in Forschung und Entwicklung (FuE) angemessen reagieren zu können. Wichtige Elemente zur Erreichung dieses Ziels sind die Prozesse von der Projektidee bis zum Projektstart zu verkürzen, Kooperationen mit weiteren Initiativen zu verstärken und eine digitale ITEA 3-Roadmap einzuführen. Durch die Neuerungen werden der bottom-up-Ansatz forciert und Innovationen erleichtert. Seit Mitte 2011 laufen die Vorbereitungen für ITEA 3 von Industrievertretern in Abstimmung mit nationalen Behörden.

Schnelllebige Zeit macht Dynamik notwendig

Um in Zukunft adäquat auf den ständigen Wandel in FuE reagieren zu können, wird ITEA 3 die Prozesse von der Idee bis zum Projektstart auf zehn Monate herabsetzen. Der zeitliche Ablauf eines ITEA 3-Calls mit den entsprechenden Einreichungsfristen wird daran angepasst werden.

Die Basis für die Ausschreibung von Projekt-Calls wird auch weiterhin eine ITEA-Roadmap sein, die aber ab 2014 in Form eines digitalen Dokuments von Experten kontinuierlich aktualisiert werden wird. Die digitale Roadmap soll es den in ITEA aktiven Partnern ermöglichen, Themen von geförderten FuE-Projekten und den Zeitraum für die dafür benötigten Investitionen flexibel mitzugestalten. Ziel dieser *Living-Roadmap* ist es, ein immer aktuelles Dokument bereitzustellen; im Gegensatz zu bisherigen statischen Dokumenten, die typischerweise in Jahresabständen überarbeitet werden. Inhaltlich greift die Living Roadmap wichtige gesellschaftliche Herausforderungen auf und stellt den von beteiligten Experten abgestimmten Stand der Technik dar. Die ITEA 3-Roadmap erfüllt zwei zentrale Anliegen: Sie ist das wichtigste Instrument zur Steuerung von Innovationen in ITEA und dient im Evaluierungsprozess als Referenzdokument, da für die Gutachter der jeweils aktuelle Stand der Technik in der Roadmap verfügbar ist und sie diesen mit den Projekt-(Zwischen-) Ergebnissen abgleichen können. Am Ende eines ITEA 3-Projektes wird der Innovationsbericht mit den Projektergebnissen in die Roadmap integriert.

Neben der Living Roadmap und der Beschleunigung der Prozesse bis zum Projektstart, plant ITEA 3 die Beziehungen zu anderen europäischen Initiativen in ähnlichen Domänen weiter ausbauen, wie zur ARTEMIS Joint Undertaking, weiteren EUREKA-Clustern, dem im Rahmen des European Institute of Innovation & Technology (EIT) gegründeten ICT Labs und zu nationalen IKT-Kompetenzclustern.

„Der Schwerpunkt unserer Projekte liegt auf Innovationen, Business Impact und einer schnellen Nutzung von Ergebnissen“, sagt der ITEA 2-Vorsitzende Rudolf Haggenmüller. „Während des letzten Jahrzehnts hatten ITEA 2 und dessen Vorgänger ITEA einen großen Einfluss auf die europäische Industrie, die zunehmend auf IKT setzt. Das hat Europas gute Position an der Spitze innovativer FuE weltweit gefestigt. Mit ITEA 3 wollen wir das hohe Level weiter ausbauen, um sicherzustellen, dass die europäische Industrie global wettbewerbsfähig bleibt.“

Rudolf Haggenmüller, ITEA 2-Vorsitzender, beim EUREKA High Level Meeting in Budapest.

Übergang von ITEA 2 zu ITEA 3 beginnt bereits 2013

ITEA 3 wird 2014 mit der ersten Ausschreibung eines Projekt-Calls starten. Im kommenden Jahr 2013 wird das Vorgängerprogramm ITEA 2 seinen letzten Call for Projects veröffentlichen. Bei diesem letzen Call werden bereits einige der angestrebten Neuerungen eingeführt, um einen reibungslosen Übergang von ITEA 2 auf ITEA 3 zu ermöglichen (Informationen zum zeitlichen Ablauf eines ITEA 2-Calls finden Sie in *SafeTRANS News* 3/2010 auf Seite 4 sowie eine allgemeine Vorstellung des ITEA-Programms in *SafeTRANS News* 3/2009 ab Seite 10. Verfügbar unter: http://safetrans-de.org/de_newsletter.php).

Hintergrundinformationen zu ITEA

ITEA ist ein Bündnis zur Förderung von FuE-Projekten im Bereich der Software-intensiven Systeme und Dienstleistungen im Rahmen der von 40 Staaten geschlossenen EUREKA-Initiative und gehört zum Bereich ICT-Cluster (weitere EUREKA-ICT-Initiativen sind CATRENE für Nanoelektronik, CELTIC für Telekommunikation und EURIPIDES für Smart Systems). Innerhalb von ITEA hat sich seit dessen Gründung 1998 eine offene Gemeinschaft der verschiedenen an FuE-Projekten beteiligten Partner etabliert.

Die an EUREKA beteiligten Staaten haben jeweils eigene Ländervertretungen, welche Ansprechpartner für das Programm sind und die FuE-Projekte betreuen. Diese Ländervertretungen arbeiten eng mit den nationalen Behörden zusammen, da ITEA selbst keine Fördermittel vergibt, sondern ein Label für förderungswürdige Projekte. Die staatliche Förderung wird nach dem Labelprozess in den Verhandlungen zwischen den Projektpartnern mit den nationalen Behörden eines jeden beteiligten Landes bestimmt. Die Betreuung von deutschen EUREKA-Projekten, und damit auch von ITEA, übernimmt das DLR in Bonn. Das DLR unterstützt somit das Bundesministerium für Bildung und Forschung (BMBF) bei allen Aufgaben, die EUREKA betreffen. Weitere Informationen dazu können Sie auf folgender Webseite nachlesen: www.eureka.dlr.de

Mehr Informationen zum Programm finden Sie unter: www.itea2.org

Beratungen zu ITEA 3 beim EUREKA High Level Meeting, Juni 2012, in Budapest.

Mit Timing-Design die Freedom-from-Interference Anforderungen der ISO 26262 erfüllen

Wie man Mixed-Critical Systems mit der richtigen Software-Architektur gleichzeitig effizient und sicher gestaltet.

Die ISO 26262, Part 6, Clause 7, formuliert sehr strenge Anforderungen an Softwarearchitekturen von Steuergeräten sowie deren Verifikation. Dabei werden die dynamischen Aspekte wie Schedules und Echtzeitverhalten besonders betont, wie auch die unbedingte Forderung nach Freedom-from-Interference (Requirement 4.11 sowie Annex D) bei Systemen mit heterogenen Sicherheitsanforderungen (mixed-criticality). Es muss beispielsweise ausgeschlossen werden, dass ASIL-C-Software durch ASIL-B- oder A-Komponenten blockiert oder verdrängt wird (im Schedule), speziell im Fehlerfall der nieder kritischen Komponenten.

Dies führt zu völlig neuen Fragestellungen und Einschränkungen der Design-Möglichkeiten. Beispielsweise sind die in Single-criticality-Systemen etablierten Echtzeit-Überwachungs-Mechanismen wie *Deadline Monitoring* (häufigste Form von Watchdogs) nicht mehr ausreichend zur Darstellung der ISO-26262-Anforderungen nach Freedom-From-Interference. Solche Watchdogs überwachen die **Symptome** von Echtzeit-Fehlern, z.B. „Funktion X verpasst die Deadline“. Für Mixed-Criticality-Systeme müssen wir aber auch die **Ursachen** unterscheiden, und die können sehr vielfältig sein, z.B.

a) „Funktion X hat aufgrund eines Fehlers eine zu lange eigene Laufzeit“ oder

b) „eine andere Funktion Y hat einen Fehler, dadurch eine zu lange Laufzeit und bremst nun Funktion X aus“ (Interferenz).

Derartige Fragestellungen sind heute als Folge der Hochintegration in immer mehr Steuergeräteprojekten an der Tagesordnung. Für den Projekterfolg wird somit die Festlegung einer geeigneten dynamischen Software-Architektur mit ihrem Schedule essentiell. Dies beinhaltet insbesondere die Auswahl von Schedule-Prioritäten sowie die Nutzung modernerer Überwachungsfunktionen. Nur so können wir die Anforderungen an Ressourceneffizienz und Sicherheit gleichermaßen erfüllen

Prioritätenverteilung

RMS (Rate Monotonic Scheduling) ist ein einfaches, weltweit etabliertes Verfahren zur Vergabe von Schedule-Prioritäten. Häufiger ausgeführte Tasks (kleine Periode) erhalten eine höhere Priorität als seltener ausgeführte (große Periode). Beispielsweise bekommt eine 1 ms-Funktion eine höhere Priorität als eine 5 ms-Funktion. Schedules nach diesem Prinzip können sehr hohe CPU-Lasten noch zuverlässig ausführen, ohne dass Deadlines verpasst werden. Jedoch ignoriert dieses Verfahren die Forderung nach Freedom-from-Interference. Tritt z.B. in der 1ms-Funktion (z.B. ASIL-A) ein Fehler auf, etwa eine Endlosschleife, so wird die 5 ms-Funktion (z.B. ASIL-C) dauerhaft verdrängt.

Das CAPA-Verfahren (Criticality As Priority Assignment) vermeidet derartige Interferenzen, indem es die Prioritäten nach den Kritikalitätsstufen verteilt. So erhält die 5ms-ASIL-C-Funktion aus dem o.g. Beispiel eine höhere Priorität als die 1 ms-ASIL-A-Funktion. Freedom-from-Interference ist per Design sichergestellt und folgt einer Empfehlung der ISO 26262. Doch dieser Ansatz ignoriert diverse zeitliche Aspekte. Wenn z.B. die 5 ms-ASIL-C-Funktion eine Laufzeit von 2 ms aufweist (entspricht 40% CPU-Last), so wird die 1 ms-ASIL-A-Funktion ihre Deadline regelmäßig und vorhersehbar verpassen; d.h. ein CAPA Schedule ist zwar sicher, aber nicht effizient.

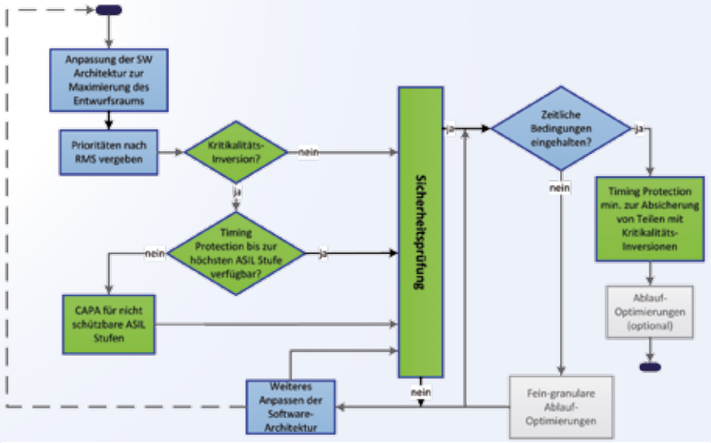
AUTOSAR Timing Protection

Um die Forderungen der ISO 26262 einzuhalten, können nun erweiterte Schutzmechanismen eingesetzt werden. Die AUTOSAR *Timing Protection* bzw. ein *Execution Time Monitoring* überwacht u.a. die Ausführungszeit (nicht die Deadline) einer Funktion oder Task während der Laufzeit. Beim Überschreiten des zugewiesenen Laufzeit-Budgets wird dies als Fehler gewertet und entsprechend konfigurierte Fehlerbehandlungsmethoden (Beenden der Funktion, Neustart des Steuergerätes) werden aktiviert. Im Vergleich zum einfachen Watchdog erfolgt die Fehlerbehandlung nun nach dem „Verursacher-Prinzip“.

Angewendet auf das obige Beispiel könnte man die 1 ms-ASIL-A-Funktion in einem effizienten RMS-Schedule von der Timing Protection überwachen lassen. Würde die Task nun in die Endlosschleife verfallen, dann würde dies sofort bemerkt und die Funktion z.B. einfach gestoppt. Eine unkontrollierte Verdrängung der 5ms ASIL-C-Funktion wird somit in jedem Fall unterbunden. Im Ergebnis erhalten wir einen hocheffizienten RMS-Schedule, der mittels Execution Time Monitoring Interferenz-frei arbeitet.

Methodik

Um die notwendigen Entscheidungen zu systematisieren, hat Symtavision zusammen mit seinen Partnern ein Vorgehensmodell entwickelt, welches bereits in der Praxis validiert wurde und in zahlreichen Projekten eingesetzt wird (Bild).



Methodik der Sicherheitsprüfung für zuverlässige Software-Architekturen in multi-kriteriellen Systemen.

Zunächst sollte ein Ablaufplan nach RMS entworfen werden, dessen Prüfung auf Kritikalitätsinversionen vergleichsweise einfach ist. Im negativen Fall wird der Entwurfsraum durch die Timing Protection erweitert. Idealerweise ist diese für die gesamte SW-Architektur verfügbar, ansonsten wird bis zum verfügbaren ASIL-Level (z.B . ist der BSW-Service *Execution Time Monitoring* heute eher selten für ASIL-C/D verfügbar) RMS und für die nicht schutzbaren ASIL-Stufen CAPA eingesetzt. Die Sicherheitsprüfung kontrolliert, ob der Schedule per Design sicher ist.

Anschließend wird die Einhaltung der zeitlichen Vorgaben geprüft. Sind diese erfüllt, wird die Timing Protection für den Schedule konfiguriert und eine optionale Optimierung für weitere Effizienzverbesserungen kann folgen. Bei Verletzung der zeitlichen Parameter sind Maßnahmen wie zum Beispiel die Anpassung der Softwarearchitektur erforderlich. Der Fehlerfall muss zusätzlich untersucht werden. Wenn beispielsweise ein gesetztes Laufzeit-Budget überschritten und die Recovery Methode gestartet wird, darf diese den Schedule nicht erneut negativ beeinflussen. Ansonsten würde zwar ein Laufzeitfehler aufgedeckt und verhindert, jedoch der Schedule durch die Fehlerbehandlung selbst gestört werden.

Um die beschriebene Optimierung bereits in einer frühen Phase der Entwicklung durchführen zu können, benötigen wir neben den typischerweise vorhandenen Konfigurationsinformationen (Tasks, Zykluszeiten, ASIL-Stufen) auch Informationen zur Ausführungszeit der Tasks bzw. Runnables. Zum Treffen grundlegender Entscheidungen sind auch grobe Abschätzungen zielführend, eine hohe Genauigkeit wird nicht benötigt.

Die vorgestellte Methodik wurde zusammen mit Kunden von Symtavision entwickelt und in der Praxis evaluiert. Ergebnis: Die Methodik erhöht die Realisierungswahrscheinlichkeit von Steuergeräte-Projekten signifikant, reduziert Sicherheitsrisiken und ermöglicht systematische Architekturoptimierungen. Gleichzeitig entsteht bei allen Beteiligten das Bewusstsein, dass Timing und Safety in Zukunft als sogenannte querschneidende Architekturaspekte sowohl beim Entwurf als auch entwicklungsbegleitend bis hin zum Test Berücksichtigung finden müssen, um die komplexen Anforderungen für die Entwicklung hochintegrierter Steuergeräte zu meistern.

Christoph Ficek, Symtavision GmbH
E-Mail: ficek@symtavision.com

Bundesministerium für Bildung und Forschung

aramis

AUTOMOTIVE · RAILWAY · AVIONICS **MULTICORE SYSTEMS**

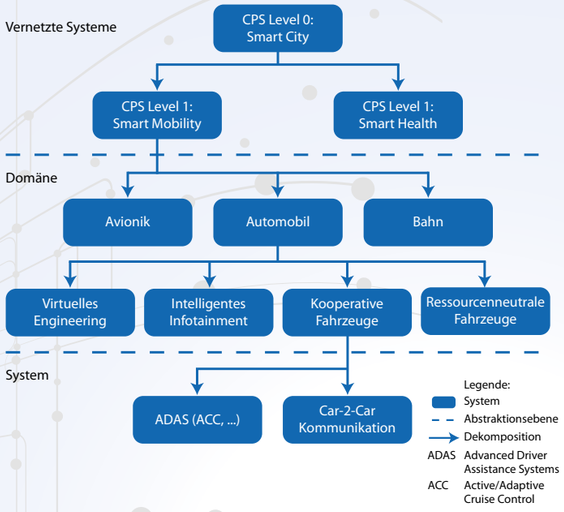
Das vom BMBF geförderte Projekt *Automotive Railway Avionics Multicore Systems* (aramis) ist im Dezember 2011 mit der symbolischen Übergabe eines Förderbescheids durch Bundesministerin Prof. Dr. Anette Schavan und dem Kick-Off des Projekts erfolgreich gestartet. aramis hat das Ziel, den breiten Einsatz von Multicore-Systemen, die hohe Anforderungen hinsichtlich Sicherheit, Zuverlässigkeit und Schutz gegen unbefugten Zugriff erfüllen müssen, vorzubereiten. Im Fokus liegen hierbei die Domänen Automobil und Avionik. Um dieses Ziel zu erreichen, vereinigt das Konsortium Kompetenzen aus allen Bereichen: Hersteller aus dem Automobil- und Flugzeugbau, deren Zulieferer, Hard- und Softwarehersteller und die auf den relevanten Gebieten renommierten Forschungseinrichtungen. Die technischen Ziele von aramis sind Hard- und Software-Architekturen sowie Methoden, welche die Entwicklung von Multicore-Systemen und Virtualisierung für Auto, Bahn und Flugzeug erlauben.

In den Teilprojekten wird aktuell zunächst eine systematische Analyse und Beurteilung des Stands der Technik auf den Ebenen System, Hardware und Software sowie Werkzeuge und Entwicklungsmethodik durchgeführt. Erste Ergebnisse lassen sich insbesondere aus dem Teilprojekt „Szenarien und Anforderungen" berichten. Dieses hat eine Basis für modellbasiertes Requirements Engineering geschaffen, die den Projektpartnern die firmen- und domänenübergreifende Zusammenarbeit ermöglicht. Des Weiteren wurde ein Systemstrukturmodell mit Abstraktionsebenen, ein Inhaltsmodell als Referenz für die Modellierung, ein gemeinsam genutztes Werkzeug-Plug-in sowie die nötige Infrastruktur zur verteilten Zusammenarbeit an einem projektübergreifenden Modell geschaffen.

Die Abstraktionsebenen (siehe Abbildung exemplarisch für Automobil) umfassen die Cyber-Physical Systems (CPS)-Ebenen mit Smart Cities und Smart Mobility, die Domänenebenen (Avionik, Automobil, Bahn), die Systemebene (z.B. Fahrerassistenzsysteme, Car-2-X, Kabinenmanagement) und die Subsystemebenen (hierarchisch, Anzahl je nach Bedarf) bis zur Software-/Hardwareebene.

In den Domänen Avionik und Automobil wurden bereits eine Reihe von Szenarien erarbeitet, deren Verfeinerung in Systemanforderungen bis Ende des Sommers vervollständigt wird. In der Domäne Automobil wurden Szenarien zu den Themen intelligentes Infotainment, kooperative Fahrzeuge, Virtual Engineering und ressourcenneutrales Fahren erstellt. Die Szenarien der Domäne Avionik betrachten die Themen Verkehrsüberwachung, Kabinenmanagement und Katastrophenmanagement. Die Domäne Bahn startet zeitlich verzögert.

Die Anteile der Szenarien und Anforderungen, welche für alle Anwendungsdomänen gelten, werden in der Domäne „Common" konsolidiert. Das betrifft vor allem Querschnittsthemen wie Nachhaltigkeit, Kontinuität und Migration. Dadurch entsteht eine wiederverwendbare Datenbasis als Referenz, die im weiteren Projektverlauf domänenübergreifend genutzt werden soll.



Mehr Informationen unter:
www.projekt-aramis.de

aramis - Übersicht

Laufzeit:	01.12.2011 - 30.11.2014
Koordinator:	Prof. Dr. Jürgen Becker, KIT Dr. Oliver Sander, KIT
Volumen:	ca. 36,5 Mio. Euro
Fördervolumen:	ca. 21 Mio. Euro
Förderung durch:	BMBF
Aufwand:	3.000 Personenmonate
Konsortium:	KIT (Koordinator)

AbsInt	Intel
Airbus	Liebherr
Audi	OFFIS
BMW	OpenSynergy
Bosch	SYMTAVISION
Continental	SYSGO
Daimler	TU Braunschweig
Diehl	TU Kaiserslautern
EADS	TU München
Elektrobit	Uni Kiel
ForTISS	Uni Paderborn
Fraunhofer	Uni Stuttgart
Freescale	Vector Informatik
Infineon	Wind River

Bundesministerium für Bildung und Forschung

SPES 2020 – Software Plattform Embedded Systems

SPES

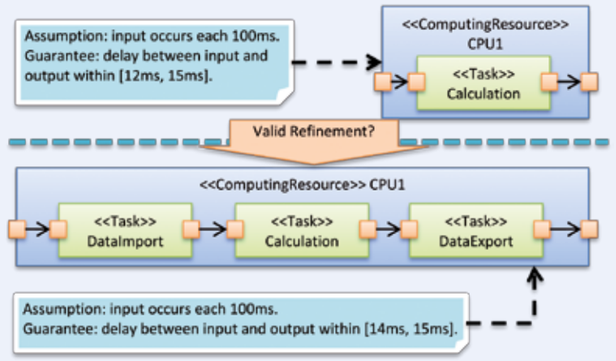
Eingebettete Systeme werden zunehmend leistungsstärker und umfassend vernetzt. Die steigenden Anforderungen an die Systeme spiegeln sich in aufwendigen Entwicklungs- und Testverfahren wider. Daher wurde das FuE-Projekt Innovationsallianz *Softwareplattform Embedded Systems 2020*, kurz SPES 2020, im November 2008 mit dem Ziel gestartet, modellbasierte Techniken und eine integrierte Werkzeugunterstützung mit einer hohen Durchgängigkeit weiterzuentwickeln. Ein bedeutendes Ergebnis des Projektes ist die Realisierung einer neuen leistungsfähige Modellierungsmethodik für die Entwicklung eingebetteter Systeme auf Basis abgestimmter Modellartefakte. Diese Modellierungsmethodik wurde bereits in einer Fallstudie bei Airbus eingesetzt und wird im Folgenden vorgestellt.

Entwurfsraum zeigt verschiedene Perspektiven des Gesamtsystems

Um der Komplexität heutiger eingebetteter Systementwicklung Rechnung zu tragen und die einzelnen Modelle im Entwicklungsprozess beherrschbar zu halten, wurde ein Modellierungsrahmenwerk entworfen. Dieser Rahmen teilt den Entwurfsraum in verschiedene Sichtweisen auf das Gesamtsystem, z.B. in Abstraktionsebenen, in Perspektiven oder in Implementierung und Spezifikation. Beim Nachweis von Systemeigenschaften wird dabei das gesamte Modell konsistent gehalten. Beispiele solcher Eigenschaften sind: Die Konsistenz der Spezifikation auf verschiedenen Dekompositionsebenen und zwischen verschiedenen Sichtweisen. Darüber hinaus sollte eine Nachvollziehbarkeit der Designentscheidungen sichergestellt werden.

Im Rahmen einer Fallstudie mit dem in SPES 2020 involvierten Partner Airbus wurde die entwickelte Modellierungsmethodik evaluiert und validiert. Als Fallstudie wählte man eine Klimaanlage zur abstrakten und ausschnittsweisen Modellierung. Anschließend wurden einige der oben angedeuteten Konsistenzeigenschaften nachgewiesen und Nachvollziehbarkeitsverbindungen zwischen Anforderungen und Verfeinerungsschritten visualisiert.

Ein Ausschnitt des Modells der Klimaanlage ist in der Abbildung unten dargestellt. Hier sieht man im oberen Teil eine abstrakte Repräsentation eines eingebetteten Prozessors mit einem Stück Software (Task), welches eine Teilberechnung der Klimaautomatik übernimmt (Berechnung der Aktoransteuerung aus Sensordaten und Stellgrößen). Im unteren Teil der Abbildung ist eine Verfeinerung dieser Task zu sehen - sie wurde in drei Tasks dekomponiert. Sowohl im oberen als auch im unteren Modell ist eine Anforderung in Form eines Contracts spezifiziert, d.h. es wird unter bestimmten Voraussetzungen das angegebene Verhalten garantiert. Die Gültigkeit dieser Verfeinerung wurde mittels der formalen Repräsentation der Anforderungen und eines Modelcheckers nachgewiesen. Weitere Details zu diesen Techniken sind z.B. in folgender Veröffentlichung ausgeführt: R. Weber et.al. A Refinement Checking Technique for Contract-Based Architecture Designs. In: S. van Baelen et.al. (Ed.). *Model Based Architecting and Construction of Embedded Systems,* LNCS 7167, Springer Verlag, 2011.



Modellausschnitt der Fallstudie auf verschiedenen Abstraktionsebenen zur Entwicklung von eingebetteten Systemen.

Allgemeines zu SPES 2020

SPES 2020 startete im November 2008 und präsentierte seine Ergebnisse bei der Abschlussveranstaltung Ende März 2012. Die wissenschaftliche Koordination des aus 21 Partnern bestehenden Projektkonsortiums hatte Prof. Dr. Dr. h.c. Manfred Broy (TU München) inne und die industrielle Leitung übernahm Dr. Reinhold Achatz (damals: Siemens AG). Das BMBF förderte SPES 2020 über die 39-monatige Projektlaufzeit mit € 22 Mio. (Gesamtkosten: € 38 Mio.).

Mehr Informationen zu SPES 2020 finden Sie unter:
http://spes2020.informatik.tu-muenchen.de

AbsInt
www.absint.com

Airbus Operations GmbH
www.airbus.de

Robert Bosch GmbH
www.bosch.de

BTC Embedded Systems AG
www.btc-es.de

Daimler AG
www.daimler.com

DB Netz AG
www.deutschebahn.com

Deutsches Zentrum für Luft- und Raumfahrt
www.dlr.de

EADS
www.eads.com

Esterel Technologies GmbH
www.esterel-technologies.com

Fraunhofer Verbund Informations- und Kommunikationstechnologie
www.iuk.fraunhofer.de

FZI
www.fzi.de

ICS AG
www.ics-ag.de

OFFIS Institut für Informatik
www.offis.de

Siemens AG
www.siemens.de

Symtavision
www.symtavion.com

TTTech
www.tttech.com

Technische Universität Braunschweig
www.tu-braunschweig.de

Universität Bremen
www.uni-bremen.de

Carl von Ossietzky Universität Oldenburg
www.uni-oldenburg.de

Verified Systems International GmbH
www.verified.de

IMPRESSUM

Herausgeber:
SafeTRANS e.V.
Escherweg 2, 26121 Oldenburg
Tel.: 0441 / 9722 540
Fax: 0441 / 9722 502
E-Mail: info@safetrans-de.org
Web: www.safetrans-de.org

Vorstand:
Prof. Dr. Werner Damm, CvO Universität Oldenburg
Dipl.-Math. Klaus Beetz, Siemens AG
Prof. Dr. Heinrich Daembkes, EADS Deutschland GmbH

Sitz des Vereins: Oldenburg (Oldb)

Vereinsregister: VR 200314
Steuernummer: 64/220/15287

Redaktion und Layout:
Franziska Böde
Escherweg 2, 26121 Oldenburg
Tel.: 0441 / 9722 540
Fax: 0441 / 9722 502
E-Mail: redaktion@safetrans-de.org

Bildmaterial:
Airbus France, BMBF, DB Netz AG, DFKI, DLR, EADS, EUREKA, ICS AG, ITEA2, KIT, OFFIS, Robert Bosch GmbH, SafeTRANS, Symatvision

Druck:
officina DRUCK Behrens Druck- und Verlags-GmbH, Oldenburg

Ausgabe:
SafeTRANS News 2/2012 werden im Juli 2012 veröffentlicht.
SafeTRANS News erscheinen dreimal jährlich und werden kostenlos abgegeben.