

NEWS



Embedded Systems - Eine Schlüsseltechnologie mit viel Zukunft



teil besitzen. Ich bin jedoch davon überzeugt, dass Schnelligkeit allein in Zukunft nicht ausreichen wird. Substanzielle Innovationen werden heute auf Systemebene erzielt. Dazu ist es erforderlich, dass die zur Zeit hervorragend spezialisierten Unternehmen gemeinsam im Sinne eines Systemansatzes tätig werden. Dies eröffnet neue Freiheitsgrade und erlaubt die Nutzung von wichtigen Synergieeffekten. Für mich bedeutet dies, dass Kooperationen innerhalb einer Branche sowie zwischen Sektoren der Schlüssel für zukünftige Erfolge sind.

vität „Centres of Innovation Excellence“ im Rahmen von ARTEMIS. Vor dem Hintergrund der starken österreichischen Zuliefererindustrie im Bereich Transport freuen wir uns Partner bei EICOSE und damit SafeTRANS zu sein.

Josef Affenzeller
ARTEMIS Austria / AVL List GmbH
Director, Research Coordination

Die Transportindustrie, insbesondere die Automobilindustrie und deren Zulieferpartner, befinden sich heute in der Phase einer technologischen Umorientierung. Ausgelöst wurde dies durch die Forderung nach Verringerung des CO₂-Ausstoßes einerseits und einer nachhaltigen Mobilität andererseits. Doch wie können wir in dieser für uns in Europa so wichtigen Industrie, die in einem globalen Umfeld notwendige Produktivität zur Erhaltung der Wertschöpfung sicherstellen?

Ein gern genutztes Argument ist, dass wir in Europa durch die Schnelligkeit in der Entwicklung einen großen Wettbewerbsvor-

Mehr und mehr komplexe Aufgaben von Systemen werden in Zukunft durch Embedded Systems, nicht nur in der Automobilindustrie sondern auch in vielen anderen Wirtschaftssektoren, gelöst. Bei Embedded Systems handelt es sich daher um wichtige Schlüsseltechnologien, deren Erfolg unmittelbar mit erfolgreichen Kooperationen verknüpft ist. Um auch in Österreich eine Vorreiterrolle bei Embedded Systems sicherzustellen, haben wir ARTEMIS Austria gegründet. Dadurch werden für Akteure in Industrie und Forschung die Awareness, Motivation und erforderlichen Rahmenbedingungen geschaffen. So unterstützt Österreich die Akti-

Inhalt

<i>Aktuelle Meldungen</i>	2
<i>Europäische Forschung ab 2014:</i>	
<i>CSF - Vorbereitung</i>	4
<i>Termine</i>	5
<i>SafeTRANS Gespräche:</i>	
<i>Prof. Rolf Ernst</i>	6
<i>SafeTRANS Mitglieder stellen sich vor:</i>	
<i>Esterel Technologies GmbH</i>	8
<i>EICOSE und E²GEST:</i>	
<i>Projektvorbereitungen</i>	10
<i>Übersicht zu Project Calls</i>	11
<i>SafeTRANS Mitglieder</i>	12

Aktuelle Meldungen

Neues aus dem Forschungs- und Wirtschaftsumfeld

Reinhart Koselleck-Projekt für Bremer Informatik

Am 1. April startete ein besonderes Forschungsprojekt an der Universität Bremen: Die Deutschen Forschungsgemeinschaft (DFG) hat Prof. Rolf Drechsler aus dem Studiengang Informatik ein Reinhart Koselleck-Projekt im Dezember 2010 bewilligt. Damit stehen dem Leiter der Arbeitsgruppe Rechnerarchitektur in den kommenden fünf Jahren 1,25 Mio. Euro zur Verfügung, um Methoden zu entwickeln, welche die Korrektheit von modernen Schaltkreis- und Systementwürfen in Eingebetteten Systemen sicherstellen.

Das Besondere der Koselleck-Projekte: Es werden wissenschaftliche Mittel für innovative, aber was die Ergebnisse angeht auch risikobehaftete Forschungsfragen bereitgestellt. Den Wissenschaftlern wird ein hohes Maß an Freiheit bei der Verwendung der Mittel zugestanden. Die wissenschaftliche Kreativität soll sich ungehindert entfalten können und nicht durch übermäßige Begeleitprüfungen eingeengt werden. Rolf Drechsler nahm die Nachricht von der Projektbewilligung begeistert auf: „Es ist ein Traum für jeden Wissenschaftler, sich über mehrere Jahre einem innovativen Projekt widmen zu können, ohne in kurzen Intervallen Ergebnisse vorweisen zu müssen. Somit sind auch größere Forschungsvorhaben realisierbar, die anspruchsvolle Vorarbeiten erfordern.“

Inhaltlich soll im Projekt eine durchgängige Methodik auf Systemebene

(electronic system level, kurz: ESL) entwickelt werden, um die zunehmende Komplexität der Systeme durch Wiederverwendung (design reuse) oder Entwurf auf höheren Abstraktionsebenen bewältigen zu können. Dabei rückt die Sicherstellung der Korrektheit der Systeme zunehmend in den Vordergrund. Der im Projekt entwickelte ESL-Verifikationsansatz soll neben den entsprechenden Verifikationsmethoden auch Verfahren zur automatischen Generierung von Eigenschaften sowie zur Überprüfung der Vollständigkeit enthalten. Die überprüften ESL-Eigenschaften werden sich zudem mit den Eigenschaften auf niedrigeren Abstraktionsebenen (z.B. auf Register-Transfer-Ebene) in Beziehung setzen lassen, so dass die Korrektheit von der Systembeschreibung bis hin zur Logikebene sichergestellt werden kann.

www.uni-bremen.de



SAFE-Projekt forscht zum ISO26262-Standard

Am 1. Juli 2011 startete das Projekt SAFE (Safe Automotive soFTware architEcture), welches Lösungen zur Demonstration von funktionaler Sicherheit im Rahmend des ISO26262-Standards unter AUTOSAR-Architektur entwickelt. Der ISO26262-Standard wird derzeit erarbeitet und voraussichtlich noch

in diesem Jahr für die Entwicklung von sicheren Automotive-Anwendungen verbindlich werden.

SAFE wird im Rahmen des europäischen Förderprogramms ITEA2 für 36 Monate unterstützt. Projektkoordinator ist die Continental Automotive GmbH. Das Projektkonsortium setzt sich aus insgesamt 24 europäischen Partnern zusammen, darunter AVL, BMW, Infineon und ZF Friedrichshafen. Das Projekt-Budget liegt bei 14 Mio. Euro.

In dem Schwesterprojekt Safe-E (Safe automotive software architecture-Enhancement), welches vom EUREKA-Programm Eurostars gefördert wird, wird seit September 2011 vorbereitend und ergänzend zu SAFE geforscht. Partner in Safe-E sind u.a. AVL-SFR, Fortiss, Infineon und TTTech.

www.safe-project.eu

Symtvision ist neues Mitglied in SafeTRANS

SafeTRANS kann seine Kooperationen mit Tool-Herstellern weiter ausbauen und festigen. Das Unternehmen Symtvision aus Braunschweig ist ab Juli 2011 Mitglied in SafeTRANS.

Symtvision entwickelt Werkzeuge zur Timing- und Scheduling-Analyse. Dazu gehören Werkzeuge und Methoden für die modellbasierte

Verifikation und Optimierung des Zeitverhaltens von Echtzeitsystemen sowie zur Visualisierung von Traces und Log-Dateien, die bei Simulationen oder Tests anfallen.

Eine Vorstellung des Unternehmens können Sie in der kommenden Ausgabe *SafeTRANS News 3/2011* lesen.

www.symtvision.com

Konferenz zu Echtzeitanalysen am 5./6. Oktober

Unter dem Motto "High time for real-time" lädt Symtvision in diesem Jahr zum fünften Mal zu seiner jährlichen News-Conference on Timing Analysis am 5. und 6. Oktober 2011 nach Braunschweig ein. Die internationale Konferenz, welche im letzten Jahr über 100 Teilnehmer aus aller Welt anzog, bietet die einmalige Gelegenheit zum Gedankenaustausch zwischen Managern, Ingenieuren, Technologieexperten und Wissenschaftlern auf dem Gebiet Eingebetteter Sicherheitskritischer Echtzeitsysteme.

Am ersten Tag, dem "Innovations Day", finden drei parallele Tracks mit Themen aus Wissenschaft und Praxis statt. Am zweiten Tag, dem „Industrial Day“, werden Experten aus verschiedenen Unternehmen wie beispielsweise Daimler, Robert Bosch oder AUDI über ihre praktischen Erfahrungen in konkreten Projekten berichten. Als Key-note-Speaker spricht Eric Bantégnie, CEO von Esterel Technologies, zum Thema „Streamlining System and Software Design with Timing Analysis“. Einzelheiten zum Programm findet man unter:

www.symtvision.com/newsconference2011.html



Rückblick: 10. Industrial Day fokussierte Referenz-Technologie-Plattformen

Um eine einheitliche und domänenübergreifende Interoperabilität von Werkzeugen für die Entwicklung von Eingebetteten Systemen zu ermöglichen, werden derzeit Referenz-Technologie-Plattformen (RTP) gemeinsam von Industrie und Wissenschaft auf nationaler und europäischer Ebene aufgebaut. In verschiedenen europäischen Forschungsprojekten werden Ansätze zur Generierung von Interoperabilität auf technischer als auch semantischer Ebene erforscht. Dazu gehört das ARTEMIS Projekt CESAR. Das Fachsymposium *SafeTRANS Industrial Day* hat sich bei seiner zehnten Veranstaltung im Mai diesen Jahres in Berlin der Entwicklung einer RTP mit Fokus auf der CESAR-RTP gewidmet. Dabei wurden verschiedene Fragestellungen und mögliche Lösungsansätze von den Experten kontrovers disku-



Eindrücke vom 10. *SafeTRANS Industrial Day*: Während der Ausstellung (oben) und einer Diskussionsrunde mit A. Keis, H. Daembkes, F. Lanteri (unten)

tiert. Bei einer Fachausstellung begleitend zum Thema konnten verschiedene Tools und Methoden, wie z.B. ein vom Fraunhofer FOKUS entwickelter ModelBus oder sich daran anschließende Werkzeuge in Funktion vorgestellt werden.

VORMERKEN: Der kommende 11. *SafeTRANS Industrial Day* wird am 8. November in Hamburg stattfinden. Mehr Informationen unter: www.safetrans-de.org/de_events.php

BTC EmbeddedTester im CESAR-Projekt

BTC Embedded Systems AG hat im Rahmen des CESAR-Projektes seine Test- und Verifikations-Werkzeugkette an den Model-Bus, eine Instanz der CESAR Reference Technology Platform (RTP), angeschlossen. Nun ist es möglich Anforderungen, welche z.B. in DOORS mit formalen Spezifikationspattern beschrieben sind, über den Model-Bus automatisch in die Verifikationsumgebung BTC EmbeddedTester zu transferieren. Die formalisierten Anforderungsspezifikationen werden dann durch BTC EmbeddedTester automatisch in C-Code-Observer synthetisiert und zur anforderungsbasierten automatisierten Testfall-Generierung, -Ausführung und -Bewertung herangezogen. Eine maximale Durchgängigkeit und Nachverfolgbarkeit ist durch die nun aufgebaute Werkzeugkette gewährleistet. BTC EmbeddedTester stellt sämtliche Interface- und Strukturinformationen sowie Testfälle im Model-Bus zur Verfügung, so dass auch andere Werkzeuge über die RTP in Zukunft angeschlossen werden können.

www.btc-es.de



Horizon 2020 wird Embedded-Forschung in Europa bestimmen

Ab 2014 wird einiges anders werden - zumindest in der europäischen Forschungsförderung. Das derzeit aktuelle 7. Europäische Rahmenprogramm für Forschung und technologische Entwicklung (FP7) läuft im Jahr 2013 aus. Über das Nachfolgeprogramm wird derzeit im *Common Strategic Framework for EU research and innovation funding*, kurz: CSF, beraten.

Dazu hat die EU ein sogenanntes „Green Paper“ als Basis für eine öffentliche Diskussion über wichtige Punkte, die beim künftigen Rahmenprogramm zur EU-Finanzierung von F&E einfließen sollten, im Februar 2011 vorgestellt. Am 10. Juni wurden Kommentare zum Green Paper und ein öffentlicher Fragenbogen über die EU-Forschungs- und Innovationsförderung auf einer Konferenz in Brüssel diskutiert. Die wichtigsten Ergebnisse umfassen:

- die Konzentration auf eine gemeinsame Strategie Europa 2020¹,
- die Bewältigung von gesellschaftlichen Herausforderungen,
- die Vereinfachung und Erleichterung des Zugangs,
- weniger Beschränkungen und Raum für kleinere Projekte um Innovation zu unterstützen und
- verstärkte bottom-up Aktivitäten.

Die Ergebnisse der Konferenz werden in die Entwicklung der Legislativvorschläge der Kommission für Forschungs- und Innovationsausgaben im Rahmen des künftigen EU-Haushalts nach 2013 eingehen. Diese Vor-

schläge werden Ende diesen Jahres vorgestellt.

Schon jetzt ist absehbar, dass CSF einen enormen finanziellen Schirm bieten kann, da sich die EU im Kontext der Strategie Europa 2020 das Ziel gesetzt hat, die Forschungsausgaben bis 2020 auf 3% des BIP zu steigern². Der konkrete Einfluss von CSF auf den Bereich der Embedded Systems-Forschung ist derzeit allerdings noch nicht absehbar. Es wird Umstrukturierungen der Instrumente und Verlagerungen der Themen geben (siehe auch Interview mit Prof. Rolf Ernst, ab Seite 6).

Auswirkungen wird CSF sicherlich auf bereits bestehende FP7-Programme im Bereich Embedded Systems-Technologien haben. Dazu gehört die Joint Technology Initiative (JTI) ARTEMIS, welche unter FP7 als Europäische Technologieplattform (ETP) startete und sich im Jahr 2008 als eine von der EU-Kommission, den Mitgliedstaaten und den industriellen Vertretern getragene Joint Undertaking (JU) etablierte. ARTEMIS veröffentlicht 2013 seinen letzten Call unter FP7 und ein Nachfolgeprogramm wird u.a. den EU-Evaluierungsbericht zu JUs von 2010 berücksichtigen und vom zukünftigen CSF beeinflusst werden.

In den Diskussionen zum CSF werden ETPs als ein wertvolles Instrument bei der Sicherung der industriellen Schwerpunkte in EU-Förderprogrammen gesehen. Im Hinblick auf leichteren Zugang wird allerdings für JTIs eine Vereinfachung von Struktur und Regeln vorgeschlagen.

Trotz laufender Beratungen zu CSF,

eines steht schon jetzt fest: Das EU-Förderprogramm für Forschung und Innovation wird *Horizon 2020 - the Framework Programme for Research and Innovation* heißen.

Eine Übersicht zu FP7-Calls im Bereich ICT in 2011/12 finden Sie auf Seite 11. Mehr zum Aufbau des aktuellen 7. Rahmenprogramms können Sie in *SafeTRANS News 2/2009* auf den Seiten 14 und 15 nachlesen (www.safetrans-de.org/de_newsletter.php).

Die Ergebnisse und Videos der öffentlichen Konsultation zum CSF finden sich auf folgender Website:

<http://ec.europa.eu/research/csfr>

¹ Mehr Informationen zu Europa 2020:

http://ec.europa.eu/europe2020/index_de.htm

² Europa 2020: Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum. Brüssel. 2010



Termine

Messen und Kongresse

10.-12.10.2011
Mikrosystemtechnik-Kongress 2011
Darmstadt
www.mikrosystemtechnik-kongress.de

16.-20.10.2011
World congress on intelligent transport systems
Orlando (USA)
www.itsa.org

18.-21.10.2011
American SAE International Aero-Tech Congress & Exhibition
Toulouse (Frankreich)
www.sae.org/events

25.-26.10.2011
ARTEMIS / ITEA Co-Summit
Helsinki, Finnland
www.artemisia-association.org
www.itea2.org

05.-08.12.2011
Embedded Software Engineering Kongress 2011
Sindelfingen
www.esk-kongress.de

Konferenzen, Tagungen und Seminare

04.-09.09.2011
ARTIST Summer School 2011
Aix-les-Bains (nahe Grenoble, FR)
www.artist-embedded.org/artist/Applications-are-open.html

13.-14.09.2011
2nd Annual Smart Grids Smart Cities Lissabon (Portugal)
<http://energy.flemingeurope.com/smart-grids-smart-cities/>

19.-21.09.2011
SAFECOMP 2011 - The 30th International Conference on Computer Safety, Reliability and Security
Neapel (Italien)
www.safecomp2011.unina.it

21.-23.09.2011
FORMATS 2011 - 9th International Conference on Formal Modeling and Analysis of Timed Systems
Aalborg (Dänemark)
<http://formats2011.cs.aau.dk/>

27.09.2011
TTA-Group Open Forum
"Safety as the Megatrend in the Embedded Industry"
Wien (Österreich)
www.ttagroup.org/openforum2011

04.-07.10.2011
9. GI Workshop Automotive Software Engineering
Berlin
www.dcaiti.tu-berlin.de/research/events/gi-ase/

05.-06.-10.2011
5th Symtvision NewsConference
www.symtvision.com/newsconference2011.html
Braunschweig

06.10.2011
9. Workshop Automotive SW Engineering – Das vernetzte Fahrzeug als Teil einer mobilen Lebenswelt
Berlin
www.dcaiti.tu-berlin.de/research/events/gi-ase/

11.-13.10.2011
it-sa - IT-Security Messe
Nürnberg
www.it-sa.de

09.-10.11.2011
9th International Conference on Embedded Security in Cars – escar
Dresden
www.escar.info

13.-15.10.2011
Int. Conference: Planning Research for the Future?
Berlin
www.fu-berlin.de/sites/inu/en/ccd/events/conference2011/conference2011.html

08.11.2011
11. SafeTRANS Industrial Day
Hamburg
www.safetrans-de.org/de_events.php

08.-09.11.2011
safetronic
München
www.hanser-tagungen.de/web/index.asp?task=001&v_id=201101201641287

22. - 24.11.2011
SPS/IPC/DRIVES 2011 – Elektrische Automatisierung - Systeme & Komponenten
Nürnberg
www.mesago.de/de/SPS/home.htm

29.-11.-02.12.2011
32nd IEEE Real-Time Systems Symposium (RTSS 2011)
Wien, Österreich
www.rtss.org

„Einheitliche Förderrichtlinien in den Ländern können das Abwandern von Ideen in Projekte verhindern“

Prof. Rolf Ernst, TU Braunschweig, über einen neuen Blick auf zukünftige Forschungsförderung und Schwerpunkte bei Architekturprinzipien

In Zukunft werden deutlich mehr Geräte das Internet nutzen als Menschen. Das Potenzial dieser Vernetzung, bei der Embedded Systems (ES) eine entscheidende Rolle spielen, bietet enorme Anwendungsmöglichkeiten, z.B. bei der Energieverteilung, medizinischen Betreuung und sicheren Mobilität. Noch sind viele der möglichen Anwendungen Zukunftsmusik. Doch gerade jetzt ist es notwendig, sich mit der Entwicklung zukünftiger ES auseinanderzusetzen. Dazu hat Professor Rolf Ernst konkrete Vorstellungen was die Forschungsthemen als auch die Forschungsförderung betrifft.

Herr Prof. Ernst, wie und wo sehen Sie ES in der zukünftigen europäischen Forschungspolitik verankert, z.B. in CSF, ARTEMIS 2 und ITEA 3?

Diese drei Programme adressieren unterschiedliche Reifegrade von Technologien. ITEA zielt auf Projekte, die relativ nah an der industriellen Verwertung sind, während sich FP7, und das zukünftige Common Strategic Framework (CSF), eher mit Vorlaufforschung beschäftigen. ARTEMIS liegt zwischen beiden Ansätzen. Dies beinhaltet u.a. die Vorbereitung von Standardisierung und die Weiterentwicklung von Technologien zur industriellen Reife.

Zukünftig wird vor allem der Beitrag zur Bewältigung von gesellschaftlichen Herausforderungen für Forschungsprojekte von ent-

scheidender Bedeutung sein. Die technischen Möglichkeiten gehen in Richtung zunehmend vernetzter und offener Systeme. Daraus ergibt sich eine neue Herangehensweise zur Förderung und industriellen Umsetzung von Ideen. Wir müssen die Dinge in Zukunft verstärkt gesellschafts- und weniger industriezentrisch sehen. Die großen, offenen Systeme werden nicht mehr nur für eine einzige Anwendung konzipiert sein, sondern einsetzbar über verschiedene Anwendungsdomänen hinweg. Konkret bei der Ausarbeitung des Nachfolgeprogramms von FP7, CSF, sehe ich die Gefahr, dass die Vorlaufforschung, die bisher in den Funding Schemes STREP und IP realisiert wird und auch Vorarbeiten zu den Programmen ITEA und ARTEMIS leistet, zu stark reduziert werden könnte. Der europäische Vorsprung, der auch mit Hilfe von guter Vorlaufforschung möglich wurde, droht verlorenzugehen. In Deutschland haben wir dafür die DFG, aber auf europäischer Ebene scheint diese Förderung nicht mehr vorgesehen zu sein. Obwohl gerade hier Industrie und Forschungseinrichtungen zusammen eine Grundidee vorantreiben können. Programme wie ARTEMIS und ITEA sind auf die Entwicklung solcher Grundideen nicht ausgerichtet. Bei diesen Programmen müssen die Basiskonzepte stehen, denn die Zeit ist zu kurz bemessen, um mit einem großen Konsortium eine neue Idee zu erarbeiten.

ARTEMIS und ITEA unterstützen eher Innovationsprojekte.

Welche Rolle werden Cyber-Physical Systems (CPS) in Forschungsprogrammen zu ES spielen?

Derzeit werden CPS unter zwei verschiedenen Definitionen betrachtet. Auf der einen Seite die deutsche Sicht, die stark von acatech favorisiert wird, welche sich hauptsächlich auf Software-intensive Systeme bezieht. Auf der anderen Seite die US-amerikanische Sicht, welche sich wahrscheinlich international durchsetzen wird, die sich hauptsächlich mit der Robustheit von unsicher vernetzten Systemen beschäftigt. Hierzu wird dringend Vorlaufforschung für ARTEMIS benötigt. CPS sollte daher definitiv ein Thema von CPS werden.

Welche Punkte sollten europäische Forschungsförderinstrumente wie ARTEMIS und ITEA2 berücksichtigen, um große Projekte, an denen viele Partner aus verschiedenen Ländern beteiligt sind, erfolgreich durchführen zu können?

Für das Gelingen von großen europäischen Projekten sind drei Bereiche besonders wichtig: die Sicherung der Projektkoordinierung, die Vereinheitlichung von länderspezifischen Richtlinien und die Abstimmung zu Verfahren und Methoden vor Projektbeginn. Zur Projektkoordinierung: Eine 100%-Förderung der Koordinierungskosten, die auf EU-Ebene aus-

gelagert werden könnte, ist eine Möglichkeit, um das Projektmanagement zu vereinfachen und die Koordinierung zu gewährleisten, auch im Falle eines Ausstiegs von Partnern auf Grund der Beschränkung von Länderbudgets. Denn die teilweise sehr große Schere zwischen Länderbudgets und Projektanträgen sowie die nationalen Länderbestimmungen machen die Förderung häufig recht unsicher. So kommen wir zum zweiten Punkt, den national unterschiedlichen Richtlinien. Diese führen, z.B. bei der Mindestbeteiligung von Industriepartnern, zu sehr heterogenen Projektkonsortien. Mit stark divergierenden Richtlinien und Länderbudgets erhöht sich das Risiko für alle Projektpartner, aber besonders für jene aus Ländern, in denen eher wenige Projekte gefördert werden, wie z.B. in Deutschland. Für diese Partner besteht die Gefahr der Abwanderung von Ideen in Projekte, aus denen man sich aufgrund nicht vorhandener Förderung zurückziehen muss. Eine Gegenmaßnahme wäre, keine Projekte zu fördern, die nur in einem kleinen Teil der beteiligten Länder bewilligt werden und bei denen der Koordinator nicht gefördert wird. Langfristig sollte auf politischer Ebene Einigkeit über ähnliche Förderrichtlinien erreicht werden.

Bezüglich der Inhalte von F&E-Projekten sollte Konsens über Grundlagentechnologien bei den Partnern herrschen, sonst droht

das Projekt auseinander zu laufen. *Wie bewerten Sie das dreiteilige Modell bei Förderinstrumenten, d.h. mit Beteiligung von EU, Nationalstaaten und Industrie, wie es in ARTEMIS umgesetzt wird?*

Der Anreiz, der von der EU ausgeht ist sehr gut und die dreiteilige Projektform hat sich in der Vergangenheit bewährt. Aber es gibt noch Möglichkeiten für Verbesserung. Dazu gehört, bürokratische Hürden abzubauen, die entstehen, wenn europäische und nationale Regeln beachtet werden müssen, die nicht immer widerspruchsfrei sind. Außerdem sollten zum Ausgleich von nationalen und europäischen Interessen Projekte ermöglicht werden, die aufgrund des thematischen Schwerpunkts nur in einzelnen Staaten angesiedelt sind. Die Vorstellung, dass viele Europäer an einem bestimmten Thema interessiert sein müssen, ist für bestimmte Ideen nicht förderlich.

In der Forschung beschäftigen Sie sich mit ES-Entwurf und -Architektur. Welche neuen Architekturprinzipien sehen Sie?

Bei Architekturprinzipien im Sinne von Eigenschaften werden Fortschritte vor allem im Bereich Mixed Criticality, Robustheit, Systemautonomie und Interoperabilität für zukünftige Systeme benötigt. Für Architekturprinzipien im Sinne mathematischer, formaler Anforderungen wird die Systemkomposition immer entschei-

Rolf Ernst



Prof. Dr.-Ing. Rolf Ernst studierte von 1976 bis 1981 Informatik an der Universität Erlangen-Nürnberg, wo er mit Auszeichnung promoviert wurde.

Forschungsaufenthalte führt ihn u.a. in die Bell Laboratories nach Pennsylvania (USA). Danach schloss sich ab 1991 die Leitung des Instituts für Datenverarbeitung an der TU Braunschweig an. Seine Forschungsschwerpunkte umfassen ES-Design und Design-Automation.

Neben zahlreichen Aktivitäten in Forschungsgremien, ist Rolf Ernst Mitglied der Europäischen Networks-of-Excellence Initiative ArtistDesign, der Deutschen Akademie der Technikwissenschaften, acatech, und Berater des BMWi im Rahmen des High-Tech-Gründungsprogramms EXIST. Rolf Ernst war in die Erstellung der ARTEMIS SRA 2011 und die Vorbereitungen zum zukünftigen Nachfolgeprogramm von FP7 (siehe Seite 4) involviert.

dender. Die formale Komposition wird künftig eine zweite Säule neben dem Test bilden, denn die Systeme gewinnen an Komplexität und öffnen sich für Kommunikations- und Vernetzungsformen, wie z.B. das Internet. Dadurch können kaum noch alle Systemeigenschaften mit einem abschließenden Test geprüft werden und man muss sich sehr viel stärker auf die Komposition verlassen können. Die Systeme werden aus Komponenten bestehen, die nach Bedarf „zusammengesteckt“ werden und Schlussfolgerungen über das Verhalten des Gesamtsystems zulassen, ohne das von Grund auf neu getestet werden muss. Diese Art der Kompositionalität wird entscheidend für die Systemintegration sein.

Vielen Dank für das Gespräch.

Modellbasierte Softwareentwicklung für sicherheitskritische Eingebettete Systeme

Esterel Technologies ist ein Softwareunternehmen, das mit den Produkten „SCADE¹ Suite“ und „SCADE Display“ Werkzeuge für die modellbasierte Entwicklung sicherheitskritischer Softwaresysteme bereit stellt, in die mehr als 10 Jahre Erfahrung in der erfolgreichen Zertifizierung von sicherheitsrelevanter Software eingeflossen sind. Dies ermöglicht dem Benutzer einen effizienten und konsistenten Prozess von der Systemspezifikation über die Validation und Verifikation bis zum Projektmanagement zu leben, und dabei Kosten und „Time to Market“ zu optimieren.

Das Unternehmen

Esterel Technologies wurde 1999 in Frankreich gegründet. Ursprünglich nur im Bereich Luftfahrt und Verteidigung aktiv, hat sich das Tätigkeitsfeld des Unternehmens in den letzten Jahren in alle Bereiche, in denen effiziente Entwicklung sicherheitsrelevanter Software eine Rolle spielt, ausgeweitet. Das umfasst neben dem Luftfahrt- & Verteidigungssektor auch die Bereiche Schienenverkehr, Energie & Nuklearerntechnik sowie Industrie und Medizin. Esterel Technologies ist inzwischen in 25 Staaten aktiv, mit mehr als 200 Kunden wie zum Beispiel Airbus, Boeing, Siemens, Liebherr und EADS. Die ISO 9001:2008 – Zertifizierung für das Design und den Verkauf von Werkzeugen und Services zur Entwicklung von Software

im sicherheitskritischen Bereich garantiert hochqualitative Produkte und Prozesse.

Herausforderungen

Die Entwicklung von Realzeitsystems, deren Versagen zu katastrophalen Folgen für Menschenleben führen kann, stellt inhärent hohe Ansprüche an den Entwicklungsprozess. Die verwendete Software muss von hoher Qualität sein und frei von Fehlern, die ein solches Versagen des Systems herbeiführen können.

Diese Ansprüche werden gesteigert durch die zunehmende Komplexität der Programme und die Tendenz, immer mehr Funktionen in Software anstatt in Hardware zu realisieren. Dies gilt insbesondere, aber nicht ausschließlich, für Mensch Maschine Interfaces (HMI).

Zusätzlich zu dem erhöhten Aufwand in der Entwicklung kommen strenge formale Auflagen für die Validation und die Verifikation solcher Softwaresysteme, die mit Hilfe traditioneller Softwareentwicklungsprozesse schwer oder gar nicht mehr beherrschbar sind, was zu komplexen und schwierigen Zertifizierungsprozessen führt, deren erfolgreicher Abschluss nicht immer garantiert ist.

Hohe Qualitätsansprüche, starke Zunahme des Funktionsumfangs und komplexe formale Auflagen führen zu einem Softwarelebenszyklus bei dem die Entwicklung bis zur Marktreife einen langen Zeitraum in Anspruch nimmt und Validierung

und Verifikation meist erst spät in den Prozess einfließen können, was zu teuren Iterationen führt.

Zusätzlich müssen im Allgemeinen mehrere Jahrzehnte Lebensdauer und auch Pflege der Produkte garantiert werden, dies stellt speziell unter Einbeziehung der Hardwareverfügbarkeit ein ganz eigenes Problemfeld dar.

Lösung

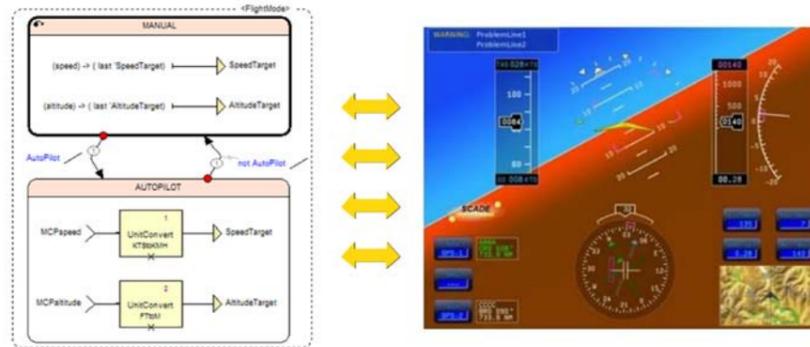
Esterel Technologies unterstützt mit der „SCADE Certified Software Factory“

Entwickler, indem den oben beschriebenen Problemen ein moderner, modellbasierter Ansatz entgegen gestellt wird, dessen Verwendung viele Schwierigkeiten traditioneller Prozesse eliminiert. Der Benutzer wird in der Realisierung und Zertifizierung von modernen Softwarelösungen, sowohl im Bereich der funktionalen Software als auch der HMI unterstützt.

Durch die Verwendung einer einfachen, formalen Sprache als Basis für die Erstellung einer Spezifikation und mächtiger Tools um Korrektheit, Fehlerfreiheit und Vollständigkeit zu garantieren, wird die

Qualität der erzeugten Produkte erhöht und bisher erst spät zu realisierende Prototyping- und Verifikationschritte können sehr viel früher in den Entwicklungsprozess eingebunden werden, was zu einer erheblichen Reduktion der Entwicklungskosten führt.

Durch automatische Codegenerierung mit einem voll qualifizierten/zertifizierten Codegenerator² wird die so getestete formale Spezifikation dann automatisch in Programmcode übersetzt, für den alle Eigenschaften gelten, die vor-



Ausschnitt aus einem Flight-Management-Modell mit SCADE SUITE erstellt und dessen visuelle Umsetzung mit SCADE DISPLAY.

her für die Spezifikation festgehalten worden sind.

Aufgrund der Plattformunabhängigkeit des generierten Programmcodes ist der Entwickler nicht mehr darauf angewiesen, sich früh im Entwicklungsprozess auf eine Plattform festzulegen und bleibt auch zu späteren Zeitpunkten flexibel in Bezug auf die gewählte Hardware. Hierdurch werden auch Probleme, die durch spätere Obsoleszenz der Hardwareplattform auftreten eliminiert.

Zusammenarbeit

In einem Markt, in dem die Projekte so komplex und vielschichtig sind, können die Anforderungen durch einen offenen Blick für Lösungen und Methoden aus verwandten Domänen bewältigt werden. Die Zusammenarbeit der Mitglieder in SafeTRANS ermöglicht den Austausch auf strategischer und technologischer Ebene über relevante Domänen hinweg. Für Esterel ist dies von großer Bedeutung, denn wir unterstützen nicht nur Kunden in der Entwicklung von Softwaresystemen, sondern arbeiten auch maßgeblich in Gremien zur Weiterentwicklung der bestehenden Standards mit (zum Beispiel DO 178C). Dadurch kann Esterel sämtliche Entwicklungen in Bezug auf geltende oder zukünftige Standards wahrnehmen und umsetzen. Dies ermöglicht es, Werkzeuge gezielt auch auf zukünftige Entwicklungen des Marktes vorzubereiten.

¹Safety Critical Application Development Environment

²Qualifiziert nach: DO-178B Level A | Def Stan 00-56 / Zertifiziert nach: EN 50128 SIL 3/4 | IEC 61508 SIL 3 | IEC 60880 full compliance | IEC 62304 full compliance

Lothar Pfeifer, Esterel Technologies GmbH

www.esterel-technologies.com



SHORTCUTS: Esterel

Unternehmen: Esterel Technologies GmbH, 100%ige Tochter der Esterel Technologies S.A.
Gründung: 1999 in Frankreich
Unternehmenssitz: D: Ottobrunn, F: Paris, Toulouse, Nizza
Mitarbeiter: D: 7, weltweit: 130
Geschäftsfelder: Herstellung und Vertrieb von Softwaretools zur modellbasierten Entwicklung von eingebetteter Software im sicherheitskritischen Bereich



Fragen an Tobias Knostmann, V.P. Central European Operations:

Esterel arbeitet in Domänen, die höchste Anforderungen an die Systemsicherheit stellen. Welche zukünftigen weiteren Anwendungsbereiche sieht Esterel für seine Produkte?

Nachdem unsere Werkzeuge in den Bereichen Aerospace & Defense, Rail und Industry schon sehr erfolgreich eingesetzt werden, sehen wir sicherlich in den Sparten Automotive und Medizintechnik für uns interessante Einsatzmöglichkeiten, da sich hier zur Zeit sehr fordernde Entwicklungsstandards etablieren, die wir von Haus aus direkt unterstützen können.

Welche vorhandenen Methoden kann man in diese neuen Bereiche übertragen?

Auch wenn Entwicklungsstandards anders heißen und verschiedene Aspekte in den Vordergrund gestellt werden, ist eine Forderung immer universell: höchstmögliche Qualität des Produkts und damit der Software. Die Methodik der modellbasierten Entwicklung mit zertifizierten Codegeneratoren ist eine universelle Antwort auf diese Forderung.

Welche Bedeutung haben Forschungsprojekte für Esterel?

Esterel ist zur Zeit in sieben verschiedenen Forschungsprojekten auf EU-Ebene tätig, unter anderem war Esterel federführend im INTERESTED-Projekt, welches im März 2011 erfolgreich im Rahmen der ICT-Förderung von FP7 beendet wurde. Diese Aktivitäten haben höchsten Stellenwert für die partnerschaftliche Erweiterung unserer Möglichkeiten und sind der Grund für unsere SafeTRANS-Mitgliedschaft.



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.symtavision.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
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:
AVL LIST GmbH, Esterel Technologies GmbH,
SafeTRANS, TU Braunschweig

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

Ausgabe:
SafeTRANS News 2/2011 werden im Juli 2011 veröffent-
licht.
SafeTRANS News erscheinen dreimal jährlich und
werden kostenlos abgegeben.

Die Rechte für alle Beiträge in den SafeTRANS News,
auch Übersetzungen, sind dem Herausgeber vor-
behalten. Reproduktionen, gleich welcher Art, ob
Fotokopie, Mikrofilm oder Erfassung in Datenver-
arbeitungsanlagen, sind nur mit schriftlicher Genehmi-
gung des Herausgebers und vollständiger Quellenan-
gabe erlaubt. Bei der Weiterleitung zu Inhalten von
Dritten übernimmt SafeTRANS für diese Inhalte keine
Verantwortung.