Hubert B. Keller, Erhard Plödereder,

Peter Dencker, Herbert Klenk (Hrsg.)

Automotive – Safety & Security 2010
Sicherheit und Zuverlässigkeit für automobile Informationstechnik

22. und 23. Juni 2010

Stuttgart

Veranstalter:

Gesellschaft für Informatik mit den Fachgruppen Ada,
ASE, ENCRESS, EZQN

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik
mit dem FA 5.11 Embedded Software

In Kooperation mit Ada Deutschland

Shaker Verlag
Aachen 2010

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Printed in Germany.

ISBN 978-3-8322-9172-3
ISSN 1433-9986

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • E-Mail: info@shaker.de

Vorwort der Herausgeber

Wie wichtig das Thema der Zuverlässigkeit von Automotive Software und Systemen ist, haben die Schlagzeilen der vergangenen Monate bewiesen. Dass wiederholtes Fehlversagen in sicherheitskritischen Komponenten im Automobil auftritt und hierdurch in Kürze ein signifikanter Marktanteil verloren gehen kann, den man sich in vielen Jahren vielleicht mühevoll über faszinierende Funktionalität oder die Qualität früherer Produkte aufgebaut hat, demonstriert eindrücklich auch die ökonomische Bedeutung, die der Zuverlässigkeit und Sicherheit dieser Systeme zukommt. Gleichzeitig werden Mechatronik, Informations- und Kommunikationstechnik sowie Informatik in rapide zunehmendem Maß die treibenden Innovationsfaktoren im Automobilbau. Kaum ein Subsystem im modernen Fahrzeug ist noch nicht durchdrungen von diesen Technologien. Die Gesellschaft für Informatik (GI) verlautet, dass 90 % aller Innovationen im Automobil Informatikbezug haben. Auch namhafte deutsche Automobilhersteller zitieren ähnlich hohe Anteile. Fortschritte in den Techniken der Sensorfusion sowie der umweltbezogenen Informationsverarbeitung und Aktorik werden uns in den kommenden Jahren visionäre Möglichkeiten an neuer Funktionalität und auch Effizienzsteigerungen im Automobil eröffnen.

Aber werden wir die wachsende Komplexität der stark vernetzten Systeme in den Griff bekommen? Und werden wir die Systeme bei den unvermeidlich vorhandenen Fehlern robust genug, also z. B. fehlertolerant gestalten können, sodass die Fahrzeuge diese Fehler zwar diagnostizieren und für die Wartungsingenieure protokollieren, die Sicherheit der Passagiere und anderer Verkehrsteilnehmer aber jederzeit gewährleistet ist und das Fahrverhalten weitestgehend unbeeinträchtigt bleibt? Fortschritte entlang all dieser Dimensionen lassen uns hoffen, dieses Ziel mittelfristig erreichen zu können. Allerdings ist zu beachten, dass sich Safety und Security Aspekte wechselseitig beeinflussen und als Gesamteigenschaft eines Systems aufgefasst werden müssen. Betriebssicherheit und Systemsicherheit haben jeweils für sich einen hohen Stand erreicht. Jetzt gilt es beide Standards gemeinsam für die sich vernetzenden Softwarekomponenten im Automobil einzubringen. Allerdings wird dieses Ziel nicht ohne Mehrkosten für Redundanz oder zusätzlicher Leistung für Plausibilitätsprüfungen, kryptographische Verfahren etc. im laufenden Betrieb erreichbar sein. Grundsätzlich ist aber festzuhalten, dass Methoden des Software Engineering Einzug in die Labore der Industrie gehalten haben. Initiativen wie AutoSAR, MISRA oder die europäische und weltweite

Normenarbeit zu einschlägigen Themen aller Phasen der Software Entwicklung, der Qualitätssicherung und der Vermeidung von Systemversagen treiben den gemeinsamen Fortschritt und auch das Wissen der Experten in Industrie, Forschung und Akademia voran. Dazu ist der Austausch dieses Wissens, der Erfahrungen, der Erfolge aber auch der erlebten Fehlschläge unbedingte Voraussetzung. In Workshops und Konferenzen wie unserer kann dieser notwendige Austausch sowohl auf dem Podium, aber vielleicht noch mehr über einem guten Glas badischen oder württembergischen Weins erfolgen.

Die Tagung "Automotive - Safety and Security 2010" stellt als 4. Veranstaltung dieser Reihe wiederum das deutsche Forum für alle Bereiche der Softwareherstellung zur Erreichung einer höheren Zuverlässigkeit in eingebetteten Systemen dar. Dass 2011 die ISO Norm 26269 für die gesamte Automobilindustrie verbindlich werden soll, zeigt den rapiden Fortschritt auf diesem Gebiet, wurde eine Orientierung an Sicherheitsnormen doch noch bei der Tagung 2004 eher als eine kostspielige Eigenart der Luftfahrtindustrie gesehen. Auch Themen der Datensicherheit und des Datenschutzes haben ihren Weg aus den Forschungslabors in die Realität zukünftiger Systeme im Automobil gefunden.

Die Tagung präsentiert sich 2010 in einem neuen Umfeld. Die Tagungen "Automotive - Safety and Security 2010“ und „International SPICE Days“ haben sich unter dem Dach des Open Forum zu einer gemeinsamen Ausrichtung zusammen gefunden. Während letztere Veranstaltung die wichtigen Aspekte der Projektdurchführung behandelt, konzentrieren wir uns wiederum auf die technische Aspekte für die Zuverlässigkeit und Sicherheit der Systeme und insbesondere der Software.

Für die gemeinsamen Hauptvorträge der beiden Konferenzen konnten wir sehr namhafte Persönlichkeiten gewinnen: Tom DeMarco, der seit Jahrzehnten zu den führenden Namen des Software Engineering zählt, Bjarne Stroustrup, der Vater von C++ und damit der Programmiersprache, die für die heute hergestellte automotive Software hochrelevant ist, Bernd Hindel, der SPICE in der Normung vorangetrieben hat, und Harald Heinecke, der die Vorausentwicklung der IT bei BMW leitend ausrichtet.

Das Tagungsprogramm 2010 umfasst neben diesen eingeladenen Hauptvorträgen ausgewählte technische Beiträge, sowie eine Ausstellung mit Präsentation von Werkzeugen zur Softwareentwicklung für das Automobil. Die Begutachtung der eingereichten Beiträge wählte knapp die Hälfte der eingereichten Beiträge für die Tagung und den vorliegenden Tagungsband aus, mit

dem wir eine bleibende Bestandsaufnahme zum Thema der Zuverlässigkeit eingebetteter Systeme insbesondere im Bereich des Automobilbaus schaffen wollen. Den Gutachtern aus dem Programmkomitee sei an dieser Stelle für ihre Arbeit gedankt.

Erstmals ergänzen wir die Konferenz mit Tutorien. Auch hierfür konnten wir Bjarne Stroustrup gewinnen, der in zwei Halbtagstutorien die richtige Verwendung von C++ in eingebetteten Systemen vermittelt. Die begleitende Ausstellung hat die Vielfalt der Methoden und Werkzeuge im Automotive Software Sektor eindrucksvoll dargestellt und den Informationsaustausch nachhaltig unterstützt.

Die gemeinsame Abendveranstaltung für alle beteiligten Konferenzen bietet den Teilnehmenden in einer entspannten und doch festlichen Atmosphäre die Möglichkeit, Kolleginnen und Kollegen kennen zu lernen, zu fachsimpeln oder auch die persönlichen Kontakte zu pflegen. Gunther Dueck, als renommierter Mathematiker, IBM Fellow und Buchautor bekannt, sorgt mit gewohnt spitzer und doch unterhaltsamer Zunge für eine geistige Bestandsaufnahme der Zunft.

Wir danken allen Partnern dieser gemeinsamen Konferenzdurchführung, voran der Wirtschaftsförderung Region Stuttgart, für ihre Unterstützung bei der Durchführung unter dem Dach des Open Forum. Wir danken den diese Konferenz fachlich mitveranstaltenden Organisationen, der Gesellschaft für Informatik (GI), der Gesellschaft für Mess- und Automatisierungstechnik im VDI/VDE (GMA), beide in Kooperation mit Ada Deutschland, sowie der Fachgruppe "Evaluation, Zertifizierung, Qualitätssicherung, Normung" (FG EZQN), dem European Network of Clubs for Reliability and Safety of Software (FG ENCRESS), der Fachgruppe "Automotive Software Engineering" (FG ASE), der Fachgruppe "Ada" und dem VDI/VDE GMA Fachausschuss 5.11 "Embedded Software" (FA 5.11 ES). Insbesondere danken wir auch den Sponsoren dieser Konferenz, deren Beitrag half, das Ambiente der Konferenz und ihren Erinnerungswert zu steigern.

Stuttgart/Karlsruhe, im Juni 2010

gez. Hubert Keller, Erhard Plödereder

Veranstalter und Sponsoren der Veranstaltung

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik

http://www.vdi.de/gma/fa5.11

GMA FA 5.11 "Embedded Software"

FG "Sicherheit - Schutz und Zuverlässigkeit"

http://www.gi-ev.de/gliederungen/fachbereiche/sicherheit/

FG "Softwaretechnik"

http://www.gi-ev.de/gliederungen/fachbereiche/softwaretechnik/

FG ADA

http://www.ada-deutschland.de/gifa/

FG ASE

http://www.gi-ev.de/fachbereiche/softwaretechnik/ase/

FG ENCRESS

http://www11.informatik.uni-erlangen.de/Encress/

FG EZQN

http://m-chair.net/gi_sicherheit_ezqn.html

Wirtschaftsförderung Region Stuttgart

http://wrs.region-stuttgart.de

Förderverein Ada Deutschland e.V.

Förderverein Ada-Deutschlkand E.v.

http://www.ada-deutschland.de

Wissenschaftliche Leitung

Dr. Hubert Keller
Karlsruher Insitut für Technologie, Institut für Angewandte Informatik,
Postfach 36 40, D-76021 Karlsruhe
Tel: 07247/82- 5756, Fax: 07247/82-5730,
E-Mail: keller@iai.fzk.de

Prof. Dr. Erhard Plödereder
Universität Stuttgart, Institut für Softwaretechnik (ISTE)
Universitätsstr. 38, D-70569 Stuttgart
Tel: 0711/7816-371, Fax: 0711/7816-220,
E-Mail: ploedere@informatik.uni-stuttgart.de

Das Organisationskomitee

Dr. Peter Dencker ETAS GmbH, Borsigstr. 14, D-70469 Stuttgart, Tel: 0711 89661-0 , Fax: 0711 89661-300 , E-Mail: peter.dencker@etas.com

Christine Harms c/o Fraunhofer Gesellschaft, Schloss Birlinghoven, D-53754 Sankt Augustin, Tel.: 02241/14-2473, Fax : 02241/14-2472, Email: christine.harms@izb.fraunhofer.de

Dr. Hubert Keller c/o Karlsruher Institut für Technologie, Institut für Angewandte Informatik, Postfach 36 40, D-76021 Karlsruhe, Tel: 07247/82- 5756, Fax: 07247/82-5730, E-Mail: keller@iai.fzk.de

Dr. Herbert Klenk EADS Deutschland GmbH, Rechliner Str. , D-85077 Manching, Tel: 08459 81-78103 , Fax: 08459 81-78604 , E-Mail: herbert.klenk@eads.com

Prof. Dr. Erhard Plödereder Universität Stuttgart, Institut für Softwaretechnik (ISTE), Universitätsstr. 38, D-70569 Stuttgart, Tel: 0711/7816-371, Fax: 0711/7816-220, E-Mail: ploedere@informatik.uni-stuttgart.de

Dr. Reha Tözun Wirtschaftsförderung Region Stuttgart, Friedrichstr. 10, D-70174 Stuttgart, Tel: 0711 22835-43, Fax: 0711 22835-55, E-Mail: reha.toezuen@region-stuttgart.de

Das Programmkomitee

Gemeinsamer Vorsitz

Hubert B. Keller, Karlsruher Institut für Technologie
Erhard Plödereder, Universität Stuttgart

Mitglieder

Andreas Bärwald, TÜV SÜD Automotive GmbH, München
Gerhard Beck, Rohde Schwarz SIT GmbH, Nellmersbach
Manfred Broy, Technische Universität München
Peter Dencker, ETAS GmbH, Stuttgart
Dirk Dickmanns, EADS, Ottobrunn
Simon Fürst, BMW Group München
Peter Göhner, Universität Stuttgart
Klaus Grimm, Daimler AG, Sindelfingen
Erwin Großpietsch, EUROMICRO, St. Augustin
Albert Held, Daimler AG, Ulm
Thomas Kropf, Robert Bosch GmbH , Leonberg
Ulrich Lefarth, ETAS GmbH, Stuttgart
Jürgen Mottok, LaS3, Hochschule Regensburg
Hans-Christian Reuss, FKFS/IVK, Universität Stuttgart
Francesca Saglietti, Universität Erlangen-Nürnberg
Christian Scheidler, Daimler AG, Berlin
Claus Stellwag, Elektrobit Automotive GmbH, Erlangen
Hans-Jörg Wolff, ETAS GmbH, Stuttgart

Inhaltsverzeichnis