Erhard Plödereder, Hubert B. Keller, Hans von Sommerfeld,
Peter Dencker, Michael Tonndorf, Francesca Saglietti (Hrsg.)

Automotive - Safety & Security 2004
Sicherheit und Zuverlässigkeit für automobile Informationstechnik

Ada Deutschland Tagung 2004
Zuverlässige Softwaresysteme

6. und 7. Oktober 2004

Universität Stuttgart

Veranstalter:

Fachgruppe *Evaluation, Zertifizierung, Qualitätssicherung, Normung* (FG EZQN) und
European Network of Clubs for Reliability and Safety of Software (FG ENCRESS)
in Kooperation mit Ada Deutschland

Shaker Verlag
Aachen 2004

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

Printed in Germany.

ISBN 3-8322-3283-4
ISSN 1433-9986

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

Vorwort

Der Workshop "Automotive – Safety & Security 2004" ist eine Initiative des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI) und der drei GI Fachgruppen Ada, EZQN (Evaluierung, Zertifizierung, Qualitätssicherung, Normung) und ENCRESS (European Network of Clubs for Reliability and Safety of Software). Angesichts des rapiden Zuwachses der Komplexität der automobilen IT und der daraus resultierenden Probleme für die Sicherheit und Zuverlässigkeit der Fahrzeuge sehen die Mitglieder dieser Organisationen die Notwendigkeit einer intensiven Auseinandersetzung mit der Thematik.

Das geschätzte Markvolumen für elektronische Bauelemente in PKWs soll im Jahre 2010 3,36 Mrd. Euro betragen. Informations- und Kommunikationselektronik bzw. elektronische Systeme haben heute schon einen Anteil von etwa 80% am deutschen Export. Damit verbunden ist die Software eine der wichtigsten aktuellen Mehrwerttechnologien. Umso stärker ist die Notwendigkeit einer hohen Zuverlässigkeit eben dieser Software. Im KFZ-Bereich sind viele Funktionalitäten ohne Software nicht oder nur mit extremem Aufwand realisierbar. Damit kommt der Software im Automobil als Teil von „embedded systems“ die tragende Rolle zu.

Dabei reicht es nicht aus, hochzuverlässige Software zu entwickeln; vielmehr muss ein nachvollziehbarer Nachweis der erzielten Zuverlässigkeit erbracht werden. Zu diesem Zweck wird auch in der Automobilindustrie an internationalen Regelwerken gearbeitet, die die Definition einheitlicher und transparenter Qualitätssicherungsprozesse als Gegenstand haben.

Mit dem Workshop "Automotive – Safety & Security 2004" soll, wie auch der deutsche Untertitel besagt, ein Forum geschaffen werden, in dem sich die Fahrzeugindustrie und Forschungsinstitute zu einem regen Wissens- und Erfahrungsaustausch auf den Gebieten der Sicherheit und Zuverlässigkeit für automobile Informationstechnologie treffen. Es freut uns daher besonders, dass bei den eingereichten und angenommenen Beiträgen ein ungewöhnlich hoher Anteil an Industriebeiträgen speziell aus dem Kfz-Bereich zu finden ist.

Der Tagungsort Stuttgart ist eines der großen Zentren des Automobilbaus in Deutschland, dank namhafter Automobilhersteller und ihrer zahlreichen großen und kleinen Zulieferfirmen, die im weiteren Umkreis von Stuttgart angesiedelt sind. Stuttgart ist damit ideal, um eine möglichst große und heterogene Gruppe der diversen Stakeholders in der automobilen IT für zwei konzentrierte Tage zusammen zu bringen, um ihre Erfahrungen auszutauschen und Wissen zu gewinnen, um den Herausforderungen begegnen zu können, Sicherheit und Zuverlässigkeit in der automobilen IT zu verbessern.

Wir alle, ob wir als Fahrer oder als Fußgänger täglich unterwegs sind, sollten an nachweisbar hochzuverlässiger Software im Auto und damit auch an den Ergebnissen dieser gemeinsamen Tagung besonders interessiert sein.

Es bot sich an, den Workshop in Ort und Zeit mit der jährlich stattfindenden Ada Deutschland Tagung zu verbinden, da die Thematik dieser Tagung ebenfalls deutlich von der Thematik zuverlässiger Softwaresysteme geprägt ist, einem Anwendungsbereich, in der speziell bei

sicherheitskritischen Systemen die Ada Technologie seit jeher eine anerkannt erfolgreiche Alternative zu anderen Programmiersprachen ist. Diese Erwägung wurde auch durch die eingereichten Beiträge bestätigt, die zum Teil beiden Veranstaltungen gleichermaßen zugeordnet werden konnten. Daher beschloss das Programmkomitee auch, die Präsentationen noch enger zu integrieren und ein gemeinsames Programm zu formulieren, das erst im letzten Viertel den Schwerpunkt in der Ada-Technologie hat.

Die angenommenen Beiträge der Tagung demonstrierten, dass jenseits der funktionalen Ausprägung der Software wesentliche Maßnahmen nötig sind, um den Anforderungen an Sicherheit und Zuverlässigkeit der Software im Kfz gerecht zu werden. Einige interessante Lösungsansätze wurden dazu angeboten.

Zusätzlich zu den Präsentationen der referierten und hier im Tagungsband wiedergegebenen Papiere wurden mehrere eingeladene Vorträge gehalten.

An den Randterminen der Tagung hatten die Fachgruppen Gelegenheit, ihre regulären Sitzungen abzuhalten.

Die Veranstaltung wurde freundlicherweise ideell und finanziell unterstützt vom Informatik-Forum Stuttgart e.V. der Universität Stuttgart, dem Förderverein Ada Deutschland e.V. und dem ausrichtendem Fachbereich und den Fachgruppen der Gesellschaft für Informatik e.V..

Wir danken nicht zuletzt den Mitgliedern des Programmkomitees für die geleistete Arbeit, die eingereichten Beiträge zu evaluieren und uns die Auswahl wesentlich zu erleichtern.

Stuttgart, im Oktober 2004

Das Organisationskomitee

Erhard Plödereder	Hubert B. Keller	Hans von Sommerfeld
Peter Dencker	Michael Tonndorf	Francesca Saglietti

Veranstalter und Sponsoren der Veranstaltung

Universität Stuttgart

http://uni-stuttgart.de

http://www.infos.informatik.uni-stuttgart.de

INFOS Informatik-Forum Stuttgart e.V.

GI Fachbereich Sicherheit

http://www.gi-fb-sicherheit.de

GI Fachgruppe ENCRESS (European Network of Clubs for Reliability and Safety of Software)

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

GI Fachgruppe EZQN (Evaluation, Zertifizierung, Qualitätssicherung, Normung)

http://www.gi-fb-sicherheit.de/fg/ezqn

http://www.ada-deutschland.de

GI Fachgruppe Ada und Förderverein Ada Deutschland e.V.

Das Organisationskomitee

Prof. Dr. Erhard Plödereder (Expertenbeirat Ada Deutschland)
c/o Universität Stuttgart, Fakultät Informatik, Elektrotechnik und Informationstechnik, Universitätsstr. 38, D-70569 Stuttgart, Tel. 0711 7816-371, Fax 0711 7816-220, E-Mail: ploedere@informatik.uni-stuttgart.de

Dr. Hubert B. Keller (Leitungsgremium Fachbereich Sicherheit - Schutz und Zuverlässigkeit)
c/o Forschungszentrum Karlsruhe GmbH, Institut für Angewandte Informatik, Postfach 36 40, D-76021 Karlsruhe, Tel: 07247/82 -5756, Fax: 07247/82 -5730, E-Mail: keller@iai.fzk.de

Hans von Sommerfeld (Leitungsgremium GI Fachgruppe EZQN)
c/o Rohde und Schwarz SIT GmbH, Agastr. 3, D-12489 Berlin, Tel. 030/65884-287, Fax: 030/65884-184, E-Mail Hans.von.Sommerfeld@SIT.rohde-schwarz.com

Dr. Peter Dencker (Sprecher GI-Fachgruppe Ada)
c/o Aonix GmbH, Emmy-Noether-Str. 11, D-76131 Karlsruhe,
Tel: 0721 98653-0, Fax: 0721 98653-98, E-Mail: dencker@aonix.de

Michael Tonndorf (Leitungsgremium GI-Fachgruppe Ada)
c/o CSC PLOENZKE AG, Sandstr. 7, 80335 München,
Tel.:089/5908 6576, Fax: 089/5908 6580, E-Mail: Michael.Tonndorf@csc.com

Prof. Dr. Francesca Saglietti (Steuerungsgremium ENCRESS)
Lehrstuhl für Software Engineering (Informatik 11), Martensstraße 3, D-91058 Erlangen,
Tel.09131/85-27870, Fax 09131/85-28746, E-Mail: saglietti@informatik.uni-erlangen.de

Das Programmkomitee

Volkert Barr, Die Schweizerische Post / PostFinance, Bern
Carsten Böckmann, Carmeq GmbH, Berlin
Jana Dittmann, Otto-von-Guericke-Universität Magdeburg
Michaël Friess, ACT Europe, Paris
Peter Göhner, Universität Stuttgart
Karl-Erwin Großpietsch, Fraunhofer-Gesellschaft
Christoph Jung, BMW AG, München
Hubert B. Keller, Forschungszentrum Karlsruhe
Isabel Münch, Bundesamt für Sicherheit in der Informationstechnik, Bonn
Erhard Plödereder, Universität Stuttgart
Kai Rannenberg, Johann Wolfgang Goethe-Universität, Frankfurt am Main
Manfred Reitenspieß, Fujitsu Siemens Computers, München
Francesca Saglietti, Friedrich-Alexander-Universität Erlangen-Nürnberg
Christian Scheidler, DaimlerChrysler AG, Stuttgart
Hans v. Sommerfeld, Rohde & Schwarz SIT GmbH, Berlin
Claus Stellwag, 3Soft GmbH, Erlangen

Inhaltsverzeichnis