Jürgen F. H. Winkler, Peter Dencker,
Hubert B. Keller, Michael Tonndorf (Hrsg.)

Ada Deutschland Tagung 2002

Software für sicherheitskritische Systeme

6. bis 8. März 2002

Jena

Friedrich-Schiller-Universität

Veranstalter:

Ada-Deutschland / Fachgruppe 2.1.5 Ada
der Gesellschaft für Informatik

Förderverein Ada Deutschland e.V.

Shaker Verlag
Aachen 2002

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Ada Deutschland Tagung 2002 : Software für sicherheitskritische Systeme / Jürgen F. H. Winkler et al. (Hrsg.).
Aachen : Shaker, 2002
(Berichte aus der Softwaretechnik)

ISBN 3-8265-9956-X

ISBN 3-8265-9956-X
ISSN 1433-9986

Shaker Verlag GmbH • Postfach 1290 • 52013 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • eMail: info@shaker.de

Vorwort

Vom 6. bis 8. März 2002 fand an der Friedrich-Schiller-Universität in Jena die **Ada Deutschland Tagung 2002** unter dem Thema *Software für sicherheitskritische Systeme* statt. Ausrichter waren die Fachgruppe 2.1.5 *Ada* der Gesellschaft für Informatik e.V. und der Förderverein Ada Deutschland e.V.

Neben Aspekten der Programmiersprache *Ada* selbst befasste sich die Tagung dieses Jahr auch mit den früheren Phasen der Softwareentwicklung, und zwar speziell im Hinblick auf den Entwurf **sicherheitskritischer Systeme**, die in der Regel auch Realzeit-Systeme sind. Da die Objektorientierung sich in der Praxis als sehr nützlich herausgestellt hat, dominieren mittlerweile bei den Sprachen für den SW-Entwurf solche, welche die Objektorientierung unterstützen. Weite Verbreitung hat in den letzten Jahren UML erfahren. Auch Realzeit-Systeme werden zunehmend unter Verwendung der Objektorientierung realisiert.

Der eingeladene Eröffnungsbeitrag von **Bichler** und **Schürr** diskutiert die Verwendung von UML für die Entwicklung von Realzeit-Systemen und schlägt Erweiterungen von UML für die Beschreibung von Realzeit-Systemen vor. Die Beiträge von **Thom** und von **Wachsmuth** beschäftigen sich ebenfalls mit UML und UML-Erweiterungen für Realzeit-Systeme. Darüber hinaus gehen beide noch auf die Abbildung von UML auf Ada ein. Thom gibt einen Überblick über eine solche Abbildung an, während Wachsmuth Beispiele der automatischen Generierung von Ada aus UML vorstellt.

Realzeit-Systeme sind häufig auch sicherheitskritische Systeme, bei deren Erstellung besondere Sorgfalt anzuwenden ist und bei welchen häufig ein Nachweis der korrekten Funktion gefordert wird. Der zweite eingeladene Beitrag von **Plödereder** gibt einen Überblick über Verfahren zur mechanischen Codeanalyse für die Zwecke von Validierung und Verifikation. **Freining, Kauer und Winkler** stellen die Ergebnisse eines Vergleich von drei automatisch arbeitenden Programmbeweisern vor, von denen zwei Ada und einer Pascal unterstützt. Tests sind auch ein wichtiges Verfahren für Validation und Verifikation. Der Beitrag von **Blotz et. al.** beschäftigt sich mit der automatischen Generierung von Testfällen aus einer Modellierungssprache heraus, die ähnlich zu UML ist.

Der Beitrag von **Barr** und **Montenegro** über ein Betriebssystem zur Unterstützung sicherheitskritischer Ada-Programme rundet das Thema *Ada und sicherheitskritische Software* ab.

Verfahren und Methoden zur Software-Entwicklung können in der Praxis nur dann effektiv eingesetzt werden, wenn sie durch entsprechende **Werkzeuge** unterstützt werden. Diesem Gesichtspunkt wird bei der Ada-Deutschland-Tagung schon immer dadurch Rechnung getragen, dass in einer Ausstellung Hersteller

von solchen Werkzeugen ihre Produkte präsentieren. Dieses Jahr wird der Werkzeugaspekt dadurch besonders betont, dass die Werkzeughersteller ihre Werkzeuge gezielt in Vorträgen und Demonstrationen vor dem Plenum vorstellen.

Ermöglicht wurde die Veranstaltung durch die freundliche Unterstützung von **ACT Europe, Aonix GmbH, ARTiSAN Software Tools GmbH, Polyspace, Rational Software GmbH, Friedrich-Schiller-Universität Jena und dem Förderverein Ada Deutschland e.V.** Das Organisationskomitee bedankt sich an dieser Stelle herzlich für die engagierte Unterstützung der Veranstaltung durch das lokale Organisationsteam der Universität Jena, Institut für Informatik.

Anlässlich der Tagung fanden die Mitgliederversammlungen der Fachgruppe 2.1.5 Ada der Gesellschaft für Informatik und des Fördervereins Ada Deutschland e.V. statt. Informationen zu beiden Organisationen und Ankündigungen zukünftiger Veranstaltungen finden sich unter **www.ada-deutschland.de**.

Jena, Karlsruhe und München, März 2002

Jürgen F. H. Winkler Peter Dencker Hubert B. Keller Michael Tonndorf

Für das Programm- und Organisationskomitee

Das Programm- bzw. Organisationskomitee

Prof. Dr. Jürgen F. H. Winkler (Vors. Programmkomitee und lokale Organisation) c/o Universität Jena, Institut für Informatik, Ernst-Abbe-Platz 2–4, D-07743 Jena, Tel.: 03641/946340, Fax: 03641/946302, E-Mail: winkler@informatik.uni-jena.de

Dr. Peter Dencker (Sprecher Fachgruppe 2.1.5 Ada) c/o Aonix GmbH, Durlacher Allee 95, D-76137 Karlsruhe, Tel: 0721/98653-0, Fax: 0721/98653-98, E-Mail: dencker@aonix.de

Dr. Hubert B. Keller (Vorsitzender Förderverein Ada Deutschland e.V.) c/o Forschungszentrum Karlsruhe GmbH, Inst. f. Angewandte Informatik, Postfach 36 40, 76021 Karlsruhe, Tel: 07247/82 -5756, Fax: 07247/82 -5730, E-Mail: keller@iai.fzk.de

Prof. Dr. Erhard Plödereder (Mitglied Expertenbeirat Förderverein Ada Deutschland e.V.) c/o Universität Stuttgart, Institut für Informatik, Breitwiesenstr. 20-22, 70565 Stuttgart, E-Mail: ploedere@informatik.uni-stuttgart.de

Michael Tonndorf (Stellv. Sprecher Fachgruppe 2.1.5 Ada) c/o CSC PLOENZKE AG, Öffentlicher Sektor Süd, Sandstr. 7, 80335 München, Tel.:089/5908 6576, Fax: 089/5908 6580, E-Mail: Michael.Tonndorf@cscploenzke.de

Inhaltsverzeichnis

Vorwort 5

Inhaltsverzeichnis 9

1 Objektorientierte Entwicklung eingebetteter (Echtzeit-) Systeme mit UML? **11**
Lutz Bichler, Andy Schürr, München-Neubiberg

2 Conformity! A Practical Integration of Standards - A Case for using the Unified Modelling Language (UML) with the Ada Programming Language **29**
Francis Thom, Cheltenham

3 Model-Based Software Engineering and Ada: Synergy for the Development of Safety-Critical Systems **37**
Andree Blotz, Franz Huber, Heiko Lötzbeyer, Alexander Pretschner, Oscar Slotosch, Hans-Peter Zängerl, München

4 Boss/Ada: An Open Source Ada 95 Safety Kit (A dependable open source embedded operating system for GNAT) **53**
Volkert Barr, Sergio Montenegro, Berlin

5 UML Entwurfsmuster zum Einsatz in sicherheitskritischen Systemen **67**
Klaus Wachsmuth, Karlsruhe

6 Codeanalysen **79**
Erhard Plödereder, Stuttgart

7 Ein Vergleich der Programmbeweiser FPP, NPPV und SPARK **127**
Carsten Freining, Stefan Kauer, Jürgen F. H. Winkler, Jena und München

8 Ada trifft Algebra **147**
Reinhard Siara, Eckernförde