

Lecture Notes in Computer Science
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2984

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Michel Wermelinger
Tiziana Margaria-Steffen (Eds.)

Fundamental Approaches to Software Engineering

7th International Conference, FASE 2004
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2004
Barcelona, Spain, March 29 – April 2, 2004
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Michel Wermelinger
Universidade Nova de Lisboa
Departamento de Informática
2829-516 Caparica, Portugal
E-mail: mw@di.fct.unl.pt

Tiziana Margaria-Steffen
Universität Dortmund
Fachbereich Informatik, LS V, Geb. IV
44221 Dortmund
E-mail: tiziana@ls5.cs.uni-dortmund.de

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): D.2, D.3, F.3

ISSN 0302-9743

ISBN 3-540-21305-8 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10990582 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2004 was the seventh instance of the European Joint Conferences on Theory and Practice of Software. ETAPS is an annual federated conference that was established in 1998 by combining a number of existing and new conferences. This year it comprised five conferences (FOSSACS, FASE, ESOP, CC, TACAS), 23 satellite workshops, 1 tutorial, and 7 invited lectures (not including those that are specific to the satellite events).

The events that comprise ETAPS address various aspects of the system development process, including specification, design, implementation, analysis and improvement. The languages, methodologies and tools that support these activities are all well within its scope. Different blends of theory and practice are represented, with an inclination towards theory with a practical motivation on the one hand and soundly based practice on the other. Many of the issues involved in software design apply to systems in general, including hardware systems, and the emphasis on software is not intended to be exclusive.

ETAPS is a loose confederation in which each event retains its own identity, with a separate program committee and independent proceedings. Its format is open-ended, allowing it to grow and evolve as time goes by. Contributed talks and system demonstrations are in synchronized parallel sessions, with invited lectures in plenary sessions. Two of the invited lectures are reserved for “unifying” talks on topics of interest to the whole range of ETAPS attendees. The aim of cramming all this activity into a single one-week meeting is to create a strong magnet for academic and industrial researchers working on topics within its scope, giving them the opportunity to learn about research in related areas, and thereby to foster new and existing links between work in areas that were formerly addressed in separate meetings.

ETAPS 2004 was organized by the LSI Department of the Catalonia Technical University (UPC), in cooperation with:

European Association for Theoretical Computer Science (EATCS)
European Association for Programming Languages and Systems (EAPLS)
European Association of Software Science and Technology (EASST)
ACM SIGACT, SIGSOFT and SIGPLAN

The organizing team comprised

Jordi Cortadella (Satellite Events), Nikos Mylonakis, Robert Nieuwenhuis,
Fernando Orejas (Chair), Edelmira Pasarella, Sonia Perez, Elvira Pino,
Albert Rubio

and had the assistance of TILESA OPC.

ETAPS 2004 received generous sponsorship from:

UPC, Spanish Ministry of Science and Technology (MCYT), Catalan
Department for Universities, Research and Information Society (DURSI),
IBM, Intel.

Overall planning for ETAPS conferences is the responsibility of its Steering Committee, whose current membership is:

Ratislav Bodik (Berkeley), Maura Cerioli (Genoa), Evelyn Duesterwald (IBM, Yorktown Heights), Hartmut Ehrig (Berlin), José Fiadeiro (Leicester), Marie-Claude Gaudel (Paris), Andy Gordon (Microsoft Research, Cambridge), Roberto Gorrieri (Bologna), Nicolas Halbwachs (Grenoble), Görel Hedin (Lund), Kurt Jensen (Aarhus), Paul Klint (Amsterdam), Tiziana Margaria (Dortmund), Ugo Montanari (Pisa), Hanne Riis Nielson (Copenhagen), Fernando Orejas (Barcelona), Mauro Pezzè (Milan), Andreas Podelski (Saarbrücken), Moaly Sagiv (Tel Aviv), Don Sannella (Edinburgh), Vladimiro Sassone (Sussex), David Schmidt (Kansas), Bernhard Steffen (Dortmund), Perdita Stevens (Edinburgh), Andrzej Tarlecki (Warsaw), Igor Walukiewicz (Bordeaux), Michel Wermelinger (Lisbon)

I would like to express my sincere gratitude to all of these people and organizations, the program committee chairs and PC members of the ETAPS conferences, the organizers of the satellite events, the speakers themselves, and finally Springer-Verlag for agreeing to publish the ETAPS proceedings. This year, the number of submissions approached 600, making acceptance rates fall to 25%. Congratulations to all the authors who made it into the final program! I hope that all the other authors still found a way of participating in this exciting event and I hope you will continue submitting.

In 2005, ETAPS will be organized by Don Sannella in Edinburgh. You will be welcomed by another “local”: my successor as ETAPS Steering Committee Chair – Perdita Stevens. My wish is that she will enjoy coordinating the next three editions of ETAPS as much as I have. It is not an easy job, in spite of what Don assured me when I succeeded him! But it is definitely a very rewarding one. One cannot help but feel proud of seeing submission and participation records being broken one year after the other, and that the technical program reached the levels of quality that we have been witnessing. At the same time, interacting with the organizers has been a particularly rich experience. Having organized the very first edition of ETAPS in Lisbon in 1998, I knew what they were going through, and I can tell you that each of them put his/her heart, soul, and an incredible amount of effort into the organization. The result, as we all know, was brilliant on all counts! Therefore, my last words are to thank Susanne Graf (2002), Andrzej Tarlecki and Paweł Urzyczyn (2003), and Fernando Orejas (2004) for the privilege of having worked with them.

Leicester, January 2004

José Luiz Fiadeiro
ETAPS Steering Committee Chair

Preface

This volume contains the proceedings of the seventh FASE, International Conference on Fundamental Approaches to Software Engineering.

FASE 2004 took place in Barcelona, Spain, during March 29–31, 2004, as part of the 7th European Joint Conference on Theory and Practice of Software (ETAPS), whose aims, organization, and history are detailed in the separate foreword by José Luiz Fiadeiro.

It is the goal of FASE to bring together researchers and practitioners interested in the challenges in software engineering research and practice: new software structuring and scaling concepts are needed for heterogeneous software federations that consist of numerous autonomously developed, communicating and interoperating systems. In particular, FASE aims at creating an atmosphere that promotes a cross-fertilization of ideas between the different communities of software engineering and related disciplines. New quality assurance methods are needed to guarantee acceptable standards of increasingly complex software applications. Different component paradigms are under discussion now, a large number of specification and modeling language are proposed, and an increasing number of software development tools and environments are being made available to cope with the problems. At the same time research on new theories, concepts, and techniques is under way, which aims at the development of a precise and (mathematically) formal foundation.

The presented contributions involved both pragmatic concepts and their formal foundation, leading to new engineering practices and a higher level of reliability, robustness, and evolvability of heterogeneous software. FASE comprised:

- **invited lectures** by Serge Abiteboul on *Distributed Information Management with XML and Web Services* and by Gruia-Catalin Roman on *A Formal Treatment of Context-Awareness*;
- **regular sessions** featuring 22 papers selected out of a record number of 91 submissions that ranged from foundational contributions to presentation of fielded applications; and
- **tool demonstrations**, featuring 4 short contributions selected out of 7 high-quality tool submissions.

FASE 2004 was hosted by the Technical University of Catalonia (UPC), and, being part of ETAPS, it shared the sponsoring and support described by the ETAPS Chair in the Foreword. Like ETAPS, FASE will take place in Edinburgh next year.

Warm thanks are due to the program committee and to all the referees for their assistance in selecting the papers, to José Luiz Fiadeiro for mastering the coordination of the whole ETAPS, and to Fernando Orejas and the whole team in Barcelona for their brilliant organization.

VIII Preface

Recognition is due to the technical support team: Martin Karusseit and Markus Bajohr at the University of Dortmund provided invaluable assistance to all the involved people concerning the Online Conference Service provided by METAFrame Technologies during the past three months. Finally, we are deeply indebted to Claudia Herbers for her first-class support in the preparation of this volume.

January 2004

Tiziana Margaria and Michel Wermelinger

Program Committee

Ralph-Johan Back (Åbo Akademi, Finland)
Jean Bézivin (Univ. of Nantes, France)
Maura Cerioli (Univ. di Genova, Italy)
Matthew Dwyer (Kansas State Univ., USA)
Reiko Heckel (Univ. of Paderborn, Germany)
Constance Heitmeyer (Naval Research Laboratory, USA)
Heinrich Hußmann (Ludwig-Maximilians-Univ. München, Germany)
Dan Craigen (ORA, Canada)
Serge Demeyer (Univ. of Antwerp, Belgium)
John Fitzgerald (Univ. of Newcastle upon Tyne, UK)
David Garlan (Carnegie Mellon Univ., USA)
Antónia Lopes (Univ. de Lisboa, Portugal)
Jeff Magee (Imperial College, UK)
Tiziana Margaria (Univ. of Dortmund, Germany (co-chair))
Tom Mens (Univ. de Mons-Hainaut, Belgium)
Mauro Pezzè (Univ. di Milano, Italy)
Gian Pietro Picco (Politecnico di Milano, Italy)
Ernesto Pimentel (Univ. de Málaga, Spain)
Gabriele Taentzer (Technische Univ. Berlin, Germany)
Michel Wermelinger (Univ. Nova de Lisboa, Portugal (co-chair))

Reviewers

Francesca Arcelli
Myla Archer
James M. Armstrong
Richard Atterer
Roswitha Bardohl
Luciano Baresi
Gilles Barthe
Ramesh Bharadwaj
Bart Du Bois
Victor Bos
Benjamin Braatz
Pietro Braione
Antonio Brogi
Jean Michel Bruel
Carlos Canal
Walter Cazzola
Alexey Cherchago
Michael Colon
Giovanni Denaro
Ralph Depke
Manuel Díaz
Gabriella Dodero
Fernando Dotti
Francisco Durán
Claudia Ermel
Hartmut Ehrig
Cristina Gacek
Stefania Gnesi

Paula Gouveia
Giovanna Guerrini
Ping Guo
Jan Hendrik Hausmann
Neil Henderson
Kathrin Hoffmann
Ralph Jeffords
Miguel Katrib
Paul Kelly
Markus Klein
Jochen Küster
Luigi Lavazza
Andreas Leicher
Elizabeth Leonard
Johan Lilius
Sten Loecher
Marc Lohmann
Antonio Maña
Leonardo Mariani
Vincenzo Martena
Jesús Martínez
Francisco Martins
Viviana Mascardi
Angelo Morzenti
Isabel Nunes
Julia Padberg
Alexander Petrenko
Guo Ping

Andreas Pleuss
Venkatesh P. Ranganath
Gianna Reggio
Marina Ribaudo
Robby
Simone Roettger
B.N. Rossiter
P.Y.A. Ryan
Filip Van Rysselberghe
Andrei Sabelfeld
Amer Saeed
Tim Schattkowsky
Hans Stenten
Sebastian Thöne
Davide Tosi
Antonio Vallecillo
Pieter Van Gorp
Vasco T. Vasconcelos
Hendrik Voigt
Sebastian Uchitel
Jef Wijsen
Kwok Cheung Yeung
Andy Zaidman
Steffen Zschaler
Albert Zündorf

Table of Contents

Invited Contributions

- Distributed Information Management with XML and Web Services 1
Serge Abiteboul

- A Formal Treatment of Context-Awareness 12
Gruia-Catalin Roman, Christine Julien, and Jamie Payton

Objects and Aspects

- Consistent Adaptation and Evolution of Class Diagrams during Refinement 37
Alexander Egyed

- Measuring Aspect Cohesion 54
Jianjun Zhao and Baowen Xu

- Refactoring Object-Z Specifications 69
Tim McComb

Smart Cards

- Checking Absence of Illicit Applet Interactions: A Case Study 84
*Marieke Huisman, Dilian Gurov, Christoph Sprenger,
and Gennady Chugunov*

- A Tool-Assisted Framework for Certified Bytecode Verification 99
Gilles Barthe and Guillaume Dufay

- Reasoning about Card Tears and Transactions in Java Card 114
Engelbert Hubbers and Erik Poll

Components I

- Predictable Dynamic Plugin Systems 129
*Robert Chatley, Susan Eisenbach, Jeff Kramer, Jeff Magee,
and Sebastian Uchitel*

- A Correlation Framework for the CORBA Component Model 144
Georg Jung, John Hatcliff, and Venkatesh Prasad Ranganath

- Cadena: An Integrated Development Environment for Analysis, Synthesis,
and Verification of Component-Based Systems 160
*Adam Childs, Jesse Greenwald, Venkatesh Prasad Ranganath,
Xianghua Deng, Matthew Dwyer, John Hatcliff, Georg Jung,
Prashant Shanti, and Gurdip Singh*

Security and Web Services

Actor-Centric Modeling of User Rights	165
<i>Ruth Breu and Gerhard Popp</i>	
Modeling Role-Based Access Control Using Parameterized UML Models ..	180
<i>Dae-Kyoo Kim, Indrakshi Ray, Robert France, and Na Li</i>	
Compositional Nested Long Running Transactions	194
<i>Laura Bocchi</i>	
DaGen: A Tool for Automatic Translation from DAML-S to High-Level Petri Nets	209
<i>Daniel Moldt and Jan Ortmann</i>	

Modeling and Requirements

Integrating Meta-modelling Aspects with Graph Transformation for Efficient Visual Language Definition and Model Manipulation	214
<i>Roswitha Bardohl, Hartmut Ehrig, Juan de Lara, and Gabriele Taentzer</i>	
An Operational Semantics for Stateflow	229
<i>Grégoire Hamon and John Rushby</i>	
Improving Use Case Based Requirements Using Formally Grounded Specifications	244
<i>Christine Choppy and Gianna Reggio</i>	
The GOPCSD Tool: An Integrated Development Environment for Process Control Requirements and Design	261
<i>Islam A.M. El-Maddah and Tom S.E. Maibaum</i>	

Testing

Automated Debugging Using Path-Based Weakest Preconditions	267
<i>Haifeng He and Neelam Gupta</i>	
Filtering TOBIAS Combinatorial Test Suites	281
<i>Yves Ledru, Lydie du Bousquet, Olivier Maury, and Pierre Bontron</i>	
Systematic Testing of Software Architectures in the C2 Style	295
<i>Henry Muccini, Marcio Dias, and Debra J. Richardson</i>	

Model Checking and Analysis

Optimising Communication Structure for Model Checking.....	310
<i>Peter Saffrey and Muffy Calder</i>	

Translating Software Designs for Model Checking	324
<i>Fei Xie, Vladimir Levin, Robert P. Kurshan, and James C. Browne</i>	

Enhancing Remote Method Invocation through Type-Based Static Analysis	339
<i>Carlo Ghezzi, Vincenzo Martena, and Gian Pietro Picco</i>	

Specification and Analysis of Real-Time Systems Using Real-Time Maude .	354
<i>Peter Csaba Ölveczky and José Meseguer</i>	

Components II

A Systematic Methodology for Developing Component Frameworks	359
<i>Si Won Choi, Soo Ho Chang, and Soo Dong Kim</i>	

Automating Decisions in Component Composition Based on Propagation of Requirements	374
<i>Ioana Şora, Vladimir Creţu, Pierre Verbaeten, and Yolande Berbers</i>	

Author Index	389
---------------------------	-----