

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2306

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Ralf-Detlef Kutsche Herbert Weber (Eds.)

Fundamental Approaches to Software Engineering

5th International Conference, FASE 2002
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2002
Grenoble, France, April 8-12, 2002
Proceedings



Springer

Series Editors

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

Volume Editors

Ralf-Detlef Kutsche
Herbert Weber
Technische Universität Berlin
FAK.IV Elektrotechnik und Informatik
Computergestützte Informationssysteme
Einsteinufer 17, 10587 Berlin, Germany
E-mail: {rkutsche,hweber}@cs.tu-berlin.de

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fundamental approaches to software engineering : 5th international conference ; proceedings / FASE 2002, held as part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2002, Grenoble, France, April 8 - 12, 2002. Ralf-Detlef Kutsche ; Herbert Weber (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2306)
ISBN 3-540-43353-8

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

ISSN 0302-9743

ISBN 3-540-43353-8 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 Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Christian Grosche, Hamburg
Printed on acid-free paper SPIN 10846521 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2002 was the fifth 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 5 conferences (FOSSACS, FASE, ESOP, CC, TACAS), 13 satellite workshops (ACL2, AGT, CMCS, COCV, DCC, INT, LDTA, SC, SFEDL, SLAP, SPIN, TPTS, and VISS), 8 invited lectures (not including those specific to the satellite events), and several tutorials.

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 which 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 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 2002 was organized by the Laboratoire Verimag in cooperation with

Centre National de la Recherche Scientifique (CNRS)
Institut de Mathématiques Appliquées de Grenoble (IMAG)
Institut National Polytechnique de Grenoble (INPG)
Université Joseph Fourier (UJF)
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

Susanne Graf - General Chair
Saddek Bensalem - Tutorials
Rachid Echahed - Workshop Chair
Jean-Claude Fernandez - Organization

Alain Girault - Publicity
Yassine Lakhnech - Industrial Relations
Florence Maraninchi - Budget
Laurent Mounier - Organization

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

Egidio Astesiano (Genova), Ed Brinksma (Twente), Pierpaolo Degano (Pisa), Hartmut Ehrig (Berlin), José Fiadeiro (Lisbon), Marie-Claude Gaudel (Paris), Andy Gordon (Microsoft Research, Cambridge), Roberto Gorrieri (Bologna), Susanne Graf (Grenoble), John Hatcliff (Kansas), Görel Hedin (Lund), Furio Honsell (Udine), Nigel Horspool (Victoria), Heinrich Hußmann (Dresden), Joost-Pieter Katoen (Twente), Paul Klint (Amsterdam), Daniel Le Métayer (Trusted Logic, Versailles), Ugo Montanari (Pisa), Mogens Nielsen (Aarhus), Hanne Riis Nielson (Copenhagen), Mauro Pezzè (Milan), Andreas Podelski (Saarbrücken), Don Sannella (Edinburgh), Andrzej Tarlecki (Warsaw), Herbert Weber (Berlin), Reinhard Wilhelm (Saarbrücken)

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. As organizer of ETAPS'98, I know that there is one person that deserves a special applause: Susanne Graf. Her energy and organizational skills have more than compensated for my slow start in stepping into Don Sannella's enormous shoes as ETAPS Steering Committee chairman. Yes, it is now a year since I took over the role, and I would like my final words to transmit to Don all the gratitude and admiration that is felt by all of us who enjoy coming to ETAPS year after year knowing that we will meet old friends, make new ones, plan new projects and be challenged by a new culture! Thank you Don!

January 2002

José Luiz Fiadeiro

Preface

The conference on Fundamental Approaches to Software Engineering (FASE) as one part of the European Joint Conferences on Theory and Practice of Software (ETAPS) focused on both aspects of ‘engineering’: rigor and applicability.

FASE 2002 now in its fifth year promoted the paradigm of ‘continuous software engineering’, including component-based software architecture, model and meta-model-based software engineering, and the understanding of the software process as an evolutionary process for the following reasons, as stated in the call for papers:

Large-scale information and communication infrastructures are of growing concern to industry and public organizations. They are expected to exist for an indefinite length of time, are supposed to be flexibly adjustable to new requirements, and are hence demanded to encompass evolvable software systems. This poses new challenges to 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 inter-operating systems; new software development processes are needed to enable the continuous improvement and extension of heterogeneous software federations.

Different component paradigms are under discussion now, a large number of specification and modeling languages have been proposed, and an increasing number of software development tools and environments have been made available to cope with the problems. At the same time research on new theories, concepts, and techniques is under way that aims at the development of their precise and (mathematically) formal foundation. In the call for papers, the following topics were emphasized:

- Component concepts and component-based software architectures, including practical concepts like EJB, DCOM, or CORBA
- Integration platforms and middleware systems for large-scale heterogeneous software federations
- Model-based software engineering
- Semi-formal and formal modeling and specification techniques for component-based software
- Meta-models of modeling and specification concepts
- Experience reports on best practices with component models and specifications, development tools, modeling environments, and software development kits
- Integration of formal concepts and current best-practice concepts in industrial software development

The program committee consisted of:

Egidio Astesiano (Genova, Italy)
 Christine Choppy (Paris, France)
 José Fiadeiro (Lisbon, Portugal)
 Anthony Finkelstein (London, UK)
 Marie-Claude Gaudel (Orsay, France)
 Heinrich Hußmann (Dresden, Germany)
 Ralf-Detlef Kutsche, co-chair (Berlin, Germany)
 Michael Löwe (Hannover, Germany)
 Tiziana Margaria (Dortmund, Germany)
 Narciso Martí Oliet (Madrid, Spain)
 Michaël Périn (UJF/Verimag, France)
 Herbert Weber, co-chair (Berlin, Germany)

The program committee received almost 60 papers, that were evaluated in an electronic submission and reviewing procedure. The members of the PC worked hard, as did also a number of co-reviewers, who are listed below. The PC cooperated closely with the responsible coordinator of the tool demonstration track, Peter D. Mosses. We would like to cordially express our thanks to all members of the PC and to all co-reviewers for their work.

Finally, the program committee decided to select 21 papers, and, additionally, in a different selection procedure, 4 short papers for the tool demonstrations associated with FASE. The result of the efforts of the reviewers and the PC are the proceedings in front of you, containing valuable new ideas and input to interesting and controversial discussions and further joint work in the challenging area of theory and practice of software engineering.

The invited lecture, with the aim of helping to bridge the gap between theory and practice, was delivered by Hellmuth Broda, the CTO of SUN Microsystems Inc. for Europe, Middle East, and Africa. He has agreed to give a talk on new visions and experiences concerning software architectures and software development in global infrastructures.

Finally, we would like to express our thanks to all contributors to the success of the conference, particularly to José Luiz Fiadeiro, the chairman of the ETAPS steering committee, and to Susanne Graf and her team in Grenoble for their great efforts in the ETAPS global coordination. Last but not least, a special thanks to the team at CIS/TU Berlin, helping with several aspects of the conference and, especially to Lutz Friedel, Claudia Gantzer, and Andreas Leicher for their great support in putting together the proceedings.

Referees

Anahita Akhavan
Egidio Astesiano
Didier Bert
Marius Bozga
Volker Braun
Felix Bübl
Christine Choppy
Juliane Dehnert
Giorgio Delzanno
Birgit Demuth
Mireille Ducass
Amal El-Fallah
José Fiadeiro
Anthony Finkelstein
Mike Fischer
Robert France
David de Frutos-Escrig
Falk Fuenfstueck
Marie-Claude Gaudel
Susanne Graf
Martin Grosse-Rhode
Claudia Gsottberger
Armando Haeberer
Heinrich Hußmann
Valérie Issarny
Jean-Claude Fernandez
Peter R. King
Yves Kodratoff
Ralf-Detlef Kutsche
Yassine Lakhnech
Ulrike Lechner
Y. Ledru
Andreas Leicher
Nicole Levy

Ben Lindner
Luis F. Llana-Díaz
Michael Löwe
Antonia Lopes
Tiziana Margaria
Bruno Marre
Ana Moreira
Laurent Mounier
Peter D. Mosses
Markus Nagelmann
Oliver Niese
Thomas Noll
Manuel Núñez
Narciso Martí Oliet
Aomar Osmani
Ricardo Peña
Michaël Périn
Pascal Poizat
Gianna Reggio
Simone Roettger
Michel de Rougemont
Oliver Rüthing
Sylviane R. Schwer
Jörn Guy Süß
Gabriele Taentzer
Anne Thomas
Alberto Verdejo
Frederic Voisin
Herbert Weber
Michel Wermelinger
Haiseung Yoo
Elena Zucca

Table of Contents

Formal Frameworks

| | |
|---|----|
| An Approach to Composition Motivated by <i>wp</i> | 1 |
| <i>Michel Charpentier (University of New Hampshire)</i> | |
| Compositional Verification of Secure Applet Interactions | 15 |
| <i>Gilles Barthe (INRIA Sophia-Antipolis), Dilian Gurov (Swedish Institute of Computer Science), and Marieke Huisman (INRIA Sophia-Antipolis)</i> | |
| A Generic Component Framework for System Modeling | 33 |
| <i>Hartmut Ehrig (Technische Universität Berlin), Fernando Orejas (Universidad Politècnica de Catalunya), Benjamin Braatz (Technische Universität Berlin), Markus Klein (Technische Universität Berlin), and Martti Piirainen (Technische Universität Berlin)</i> | |

Model and Program Analysis

| | |
|--|----|
| Implementing Condition/Event Nets in the Circal Process Algebra | 49 |
| <i>Antonio Cerone (University of Queensland)</i> | |
| Integrated State Space Reduction for Model Checking Executable Object-Oriented Software System Designs | 64 |
| <i>Fei Xie and James C. Browne (University of Texas)</i> | |
| Model Generation by Moderated Regular Extrapolation..... | 80 |
| <i>Andreas Hagerer (METAFrame Technologies), Hardi Hungar (METAFrame Technologies), Oliver Niese (University of Dortmund), and Bernhard Steffen (University of Dortmund)</i> | |
| Better Slicing of Programs with Jumps and Switches | 96 |
| <i>Sumit Kumar (University of Wisconsin) and Susan Horwitz (University of Wisconsin/GrammaTech)</i> | |

Architecture Descriptions

| | |
|--|-----|
| Architectural Types Revisited: Extensible And/Or Connections | 113 |
| <i>Marco Bernardo and Francesco Franzè (Università di Urbino)</i> | |

| | |
|---|-----|
| Mapping an ADL to a Component-Based Application Development Environment | 128 |
| <i>Virgínia C.C. de Paula and Thais V. Batista (University of Rio Grande)</i> | |
| From EDOC to CCM Components: A Precise Mapping Specification | 143 |
| <i>Mariano Belaunde and Mikael Peltier (France Telecom)</i> | |

Meta-Models

| | |
|--|-----|
| Engineering Modelling Languages: A Precise Meta-Modelling Approach ... | 159 |
| <i>Tony Clark (King's College), Andy Evans (Univeristy of York), and Stuart Kent (University of Kent)</i> | |
| AToM ³ : A Tool for Multi-formalism and Meta-modelling | 173 |
| <i>Juan de Lara (Universidad Autónoma de Madrid/University Montréal) and Hans Vangheluwe (University Montréal)</i> | |
| A Toolbox for Automating Visual Software Engineering | 189 |
| <i>Luciano Baresi (Politecnico di Milano) and Mauro Pezzè (Università degli Studi di Milano - Bicocca)</i> | |

Formal Approaches towards UML

| | |
|---|-----|
| Enriching OCL Using Observational Mu-Calculus | 203 |
| <i>Julian Bradfield, Juliana Küster Filipe, and Perdita Stevens (University of Edinburgh)</i> | |
| Formal Verification of UML Statecharts with Real-Time Extensions | 218 |
| <i>Alexandre David (Uppsala University), M. Oliver Möller (Aarhus University), and Wang Yi (Uppsala University)</i> | |

Requirements Engineering

| | |
|--|-----|
| An Authoring Tool for Informal and Formal Requirements Specifications .. | 233 |
| <i>Reiner Hähnle, Kristofer Johannisson, and Aarne Ranta (Chalmers University of Technology)</i> | |
| Introducing Context-Based Constraints | 249 |
| <i>Felix Bübl (Technische Universität Berlin)</i> | |
| Formal Requirements Engineering Using Observer Models | 264 |
| <i>Andreas Nonnengart, Georg Rock, and Werner Stephan (German Research Centre for Artificial Intelligence)</i> | |

| | |
|--|------------|
| Automatic Generation of Use Cases from Workflows: | |
| A Petri Net Based Approach | 279 |
| <i>Oscar López (Technological Institute of Costa Rica), Miguel A. Laguna (University of Valladolid), and Francisco J. García (University of Salamanca)</i> | |
| Meta-modeling Techniques Meet Web Application Design Tools | 294 |
| <i>Luciano Baresi, Franca Garzotto, Luca Mainetti, and Paolo Paolini (Politecnico di Milano)</i> | |
| Formal-Driven Conceptualization and Prototyping of Hypermedia Applications | 308 |
| <i>Antonio Navarro, Baltasar Fernandez-Manjon, Alfredo Fernandez-Valmayor, and Jose Luis Sierra (Universidad Complutense de Madrid)</i> | |
| <hr/> Tool Demonstrations <hr/> | |
| The Coordination Development Environment | 323 |
| <i>João Gouveia, Georgios Koutsoukos, Michel Wermelinger, Luís Andrade, and José Luiz Fiadeiro (Univ. Nova de Lisboa)</i> | |
| The K ² System: Integrating Object-Oriented Design and Formal Methods | 327 |
| <i>Wolfgang Ahrendt (Chalmers University of Technology), Thomas Baar (Universität Karlsruhe), Bernhard Beckert (Universität Karlsruhe), Martin Giese (Universität Karlsruhe), Elmar Habermalz (Universität Karlsruhe), Reiner Hähnle (Chalmers University of Technology), Wolfram Menzel (Universität Karlsruhe), Wojciech Mostowski (Chalmers University of Technology), and Peter H. Schmitt (Universität Karlsruhe)</i> | |
| ObjectCheck: A Model Checking Tool for Executable Object-Oriented Software System Designs | 331 |
| <i>Fei Xie (Univ. of Texas), Vladimir Levin (Bell Laboratories), and James C. Browne (Univ. of Texas)</i> | |
| Demonstration of an Operational Procedure for the Model-Based Testing of CTI Systems | 336 |
| <i>Andreas Hagerer, Hardi Hungar, Tiziana Margaria (METAFrame Technologies), Oliver Niese, Bernhard Steffen (University of Dortmund), and Hans-Dieter Ide (Siemens AG)</i> | |
| Author Index | 341 |