

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Tom Maibaum (Ed.)

Fundamental Approaches to Software Engineering

Third International Conference, FASE 2000
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2000
Berlin, Germany, March 25 – April 2, 2000
Proceedings



Springer

Series Editors

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

Volume Editor

Tom Maibaum
King's College London
Department of Computer Science
Strand, London WC2R 2LS, UK
E-mail:tom@maibaum.org

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fundamental approaches to software engineering : third international conference ; proceedings / FASE 2000, held as part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2000, Berlin, Germany, March 25 - April 2, 2000. Tom Maibaum (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1783)
ISBN 3-540-67261-3

CR Subject Classification (1991): D.2, D.3, F.3

ISSN 0302-9743

ISBN 3-540-67261-3 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 company in the BertelsmannSpringer publishing group.
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN 10719952 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2000 was the third 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), five satellite workshops (CBS, CMCS, CoFI, GRATRA, INT), seven invited lectures, a panel discussion, and ten 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. The program of ETAPS 2000 included a public business meeting where participants had the opportunity to learn about the present and future organization of ETAPS and to express their opinions about what is bad, what is good, and what might be improved.

ETAPS 2000 was hosted by the Technical University of Berlin and was efficiently organized by the following team:

Bernd Mahr (General Chair)
Hartmut Ehrig (Program Coordination)
Peter Pepper (Organization)
Stefan Jähnichen (Finances)
Radu Popescu-Zeletin (Industrial Relations)

with the assistance of BWO Marketing Service GmbH. The publicity was superbly handled by Doris Fähndrich of the TU Berlin with assistance from the ETAPS publicity chair, Andreas Podelski. Overall planning for ETAPS conferences is the responsibility of the ETAPS steering committee, whose current membership is:

Egidio Astesiano (Genova), Jan Bergstra (Amsterdam), Pierpaolo Degano (Pisa), Hartmut Ehrig (Berlin), José Fiadeiro (Lisbon), Marie-Claude Gaudel (Paris), Susanne Graf (Grenoble), Furio Honsell (Udine), Heinrich Hußmann (Dresden), Stefan Jähnichen (Berlin), Paul Klint (Amsterdam), Tom Maibaum (London), Tiziana Margaria (Dortmund), Ugo Montanari (Pisa), Hanne Riis Nielson (Aarhus), Fernando Orejas (Barcelona), Andreas Podelski (Saarbrücken), David Sands (Göteborg), Don Sannella (Edinburgh), Gert Smolka (Saarbrücken), Bernhard Steffen (Dortmund), Wolfgang Thomas (Aachen), Jerzy Tiuryn (Warsaw), David Watt (Glasgow), Reinhard Wilhelm (Saarbrücken)

ETAPS 2000 received generous sponsorship from:

the Institute for Communication and Software Technology of TU Berlin
the European Association for Programming Languages and Systems
the European Association for Theoretical Computer Science
the European Association for Software Science and Technology
the “High-Level Scientific Conferences” component of the European
Commission’s Fifth Framework Programme

I would like to express my sincere gratitude to all of these people and organizations, the program committee 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.

January 2000

Donald Sannella
ETAPS Steering Committee chairman

Preface

The conference on Fundamental Approaches to Software Engineering (FASE) is one of the confederated conferences within ETAPS. It aims at providing a forum where rigorous methods (in the sense used by scientists and engineers) for the software production process may be discussed. FASE is related to the correspondingly ‘acronymed’, but differently named conference that was traditionally part of the late TAPSOFT series. There is thus a tradition to uphold, but also a shift in emphasis: we wish to address issues in software engineering rigorously, but not necessarily simply mathematically. Engineers in the classical disciplines use a mixture of formal and heuristic methods in a design process, which has been legitimized by being well founded with respect to scientific and mathematical foundations, and by repeated and repeatable successes in delivering artefacts that are ‘fit for purpose’.

The call for papers stated this view as follows:

To achieve the status of a proper engineering discipline, software engineering requires engineering design and analysis METHODS which are firmly grounded on scientifically sound concepts as well as well-founded software tools and analyses based on sound engineering principles. Fundamental approaches are sought, integrating formal approaches with principled methods, providing the bridge between theory and practice and aimed at producing engineering methods and tools for the various phases of software development. FASE is intended to provide a forum where fundamental approaches to software engineering are presented, compared and discussed. Contributions should focus on the problems and methods of software engineering; papers are especially welcome on the following topics:

- Methods for the design of high quality software, relying on formal approaches to specification, refinement, testing, and validation
- The use of program derivation and transformation methods to support software production
- Integration of formal notations and methods with engineering notations and methods
- Combining programming in the small and programming in the large software architectures
- Principled approaches to reverse engineering, legacy software, reuse and evolution
- Case studies of the application of principled software engineering methods
- Reports evaluating industrial experience of the use of software engineering methods
- Rigorous experimental studies of the effectiveness and applicability of principled methods

The program committee consisted of:

Gul Agha, University of Illinois Urbana
 David Basin, Albert-Ludwigs-Universität Freiburg
 Dan Craigen, ORA Canada
 Peter Dybjer, Chalmers University of Technology
 José Luiz Fiadeiro, University of Lisbon
 Jean-Pierre Finance, University of Nancy
 Hans-Dieter Ehrich, Technical University of Braunschweig
 Heinrich Hußmann, Technical University of Dresden
 Michael Lowry, NASA Ames Research Center
 Jeff Magee, Imperial College
 Tom Maibaum (chair), King's College London
 Dino Mandrioli, Politecnico di Milano
 Narciso Martí-Oliet, Universidad Complutense Madrid
 Peter Mosses, University of Aarhus
 Andrzej Tarlecki, University of Warsaw

We received almost 60 papers and used an electronic method of review. We did not actually meet physically. This has been tried before and worked well. I believe that this was again the case. This was in no small measure due to the PC and to the referees that agreed to help them. The names of these referees are listed immediately after the preface and I would like to take this opportunity to heartily thank them all! I would also like to thank Anna Maros for her administrative help and particularly Kelly Androutsopoulos for her hard extensive efforts in making the electronic system work!

The result of all this effort is on display in this volume. I hope that you will find the 21 papers useful and inspirational. Three short papers related to tools demonstrations relevant to FASE further supplement the volume. The demonstrations were chosen using a different, global mechanism and then assigned to relevant conferences. Also, we have the contributions of 3 invited speakers assigned to this volume. The FASE invited speaker, Wlad Turski, has contributed an intriguing assessment of software engineering at the turn of the century. He looks back to the original conference 'establishing' the discipline, its focus over the last few decades, and the need to refocus our efforts in different directions so as to better support the present needs of software engineering. He ends on a somewhat pessimistic note. . . . I look forward to the discussions which I am certain will be generated at the conference.

The two 'global' invited speakers, David Harel and Richard Mark Soley, have made short contributions related to their invited talks. Harel focuses on the need to do further research on behaviour and how to represent it, a topic also taken up extensively by Turski. Soley focuses on the need to develop the capability of dynamically linking information on the Web so as to enhance our ability to find and use information.

Referees

Agha, Gul
Alexandre, Francis
Ambroszkiewicz, Stanislaw
Andrade, L.
Andreu, I. Pita
Ayari, Abdelwaheb
Baresi, Luciano
Basin, David
Baumeister, Hubert
Bednarczyk, Marek
Bidoit, Michel
Blanc, B.
Boyd, Mark
Brat, Guillaume
Craigén, Dan
Cugola, Giampaolo
Danvy, Olivier
de Frutos-Escrig, David
de Groote, Philippe
Demuth, Birgit
Duran, Francisco
Dybjer, Peter
Eckstein, Silke
Ehrich, Hans-Dieter
Festor, Olivier
Fiadeiro, José Luis
Finance, Jean-Pierre
Fischer, Bernd
Fischer, Mike
Fitzgerald, J. S.
Friedric, Stefan
Fuenfstueck, Falk
Galan Corroto, L. Antonio
Godart, Claude
Grau, Antonio
Grudzinski, Grzegorz
Havelund, Klaus
Husmann, Heinrich
Jabłonowski, Janusz
Jacquot, J. P.
Jamali, Nadeem
Jaray, Jacques
Kubica, Marcin
Kuester Filipe, Juliana

Kumichel, Frank-Ulrich
Laprie, Jean-Claude
Lasota, Sławomir
Llana-Díaz, Luis F.
Lopes, A.
Lowry, Michael
Lukaszewicz, Witold
Magee, Jeff
Maibaum, Tom
Mandrioli, Dino
Marroquin Alonso, Olga
Martí-Oliet, Narciso
Monga, Mattia
Mosses, Peter D.
Méry, Dominique
Neumann, Karl
Nipkow, Tobias
Nunes, I.
Orso, Alex
Park, Seungjoon
Pecher, Charles
Penczek, W.
Penix, John
Pinger, Ralf
Pressburger, Thomas
Roegel, Denis
Rossi, Matteo
Schumann, Johan
Segura, Clara
Sernadas, Cristina
Souquères, Jeanine
Tarlecki, Andrzej
Thati, Prasanna
Thiemann, Peter
Varela, Carlos
Verdejo, Alberto
Vigano, Luca
Visser, Willem
Wermelinger, M.
Whittle, Jonathan
Winkowski, J.
Wolff, Burkhardt
Ziaei, Reza

I want to thank Don Sannella, chair of the ETAPS steering committee for his many great efforts on behalf of the ETAPS community. The organizers in Berlin should also be thanked for their work in making the conference a great success. Finally, I would also like to thank Matt Bishop for his hard work in putting together the proceedings.

January 2000

Tom Maibaum

Table of Contents

Invited Papers

An Essay on Software Engineering at the Turn of Century	1
<i>Władysław M. Turski (Warsaw University)</i>	
Memex Is Not Enough	21
<i>Richard Mark Soley (Object Management Group)</i>	
From Play-In Scenarios to Code: An Achievable Dream	22
<i>David Harel (Weizmann Institute of Science)</i>	

Real-Time Systems

Parallel Refinement Mechanisms for Real-Time Systems	35
<i>Paul Z. Kolano (Lockheed Martin), Richard A. Kemmerer (University of California, Santa Barbara), and Dino Mandrioli (Politecnico di Milano)</i>	
Applying RT-Z to Develop Safety-Critical Systems	51
<i>Carsten Sühl (GMD FIRST)</i>	
A Process Algebra for Real-Time Programs	66
<i>Henning Dierks (University of Oldenburg)</i>	

Formally Engineering Systems

System Fault Tolerance Specification: Proposal of a Method Combining Semi-formal and Formal Approaches	82
<i>Giovanna Dondossola and Oliver Botti (ENEL)</i>	
Structuring and Design of Reactive Systems Using RSDS and B	97
<i>K. Lano, K. Androutsopoulos (King's College London), and D. Clark (Imperial College)</i>	
Using Domain-Specific Languages for the Realization of Component Composition	112
<i>Matthias Anlauff (GMD FIRST), Philipp W. Kutter (Swiss Federal Institute of Technology), Alfonso Pierantonio (Università di L'Aquila), and Asuman Sünbül (Technical University Berlin)</i>	

Software Engineering

Analysing UML Active Classes and Associated State Machines – A Lightweight Formal Approach	127
<i>G. Reggio, E. Astesiano (Università di Genova), C. Choppy (Université Paris XIII), and H. Hussmann (Dresden University of Technology)</i>	
Software as Learning: Quality Factors and Life-Cycle Revised	147
<i>José Hernández-Orallo and M^a José Ramírez-Quintana (Universitat Politècnica de València)</i>	
What Is ‘Mathematicalness’ in Software Engineering?	163
<i>Hidetaka Kondoh (Hitachi)</i>	
A Formal Approach to Heterogeneous Software Modeling	178
<i>Alexander Egyed and Nenad Medvidovic (University of Southern California)</i>	

Object Orientation

Formal Specification of Object-Oriented Meta-modelling	193
<i>Gunnar Övergaard (Royal Institute of Technology, Stockholm)</i>	
Verification of Object Oriented Programs Using Class Invariants	208
<i>Kees Huizing, Ruurd Kuiper, and SOOP (Eindhoven University of Technology)</i>	
Verification of Object-Z Specifications by Using Transition Systems: Application to the Radiomobile Network Design Problem	222
<i>Pablo Gruer, Vincent Hilaire, and Abder Koukam (Université de Technologie de Belfort Montbéliard)</i>	
A Model for Describing Object-Oriented Systems from Multiple Perspectives	237
<i>Torsten Nelson, Donald Cowan, and Paulo Alencar (University of Waterloo)</i>	

Formally Engineering Systems

Stepwise Introduction and Preservation of Safety Properties in Algebraic High-Level Net Systems	249
<i>J. Padberg, K. Hoffmann, and M. Gajewsky (Technical University Berlin)</i>	

Theory and Applications

Ready-Simulation Is Not Ready to Express a Modular Refinement Relation	266
<i>Françoise Bellegarde, Jacques Julliand, and Olga Kouchnarenko (Université Franche-Comté)</i>	

Java Program Verification via a Hoare Logic with Abrupt Termination . . .	284
<i>Marieke Huisman and Bart Jacobs (University of Nijmegen)</i>	
Foundations for Software Configuration Management Policies Using Graph Transformations	304
<i>Francesco Parisi-Presicce (Università degli Studi di Roma “La Sapienza”) and Alexander L. Wolf (University of Colorado at Boulder)</i>	
Analyzing Non-functional Properties of Mobile Agents	319
<i>Pascal Fradet, Valérie Issarny, and Siegfried Rouvrais (IRISA/INRIA)</i>	
Case Studies	
Specification of an Automatic Manufacturing System: A Case Study in Using Integrated Formal Methods	334
<i>Heike Wehrheim (Universität Oldenburg)</i>	
A Case Study on Using Automata in Control Synthesis	349
<i>Thomas Hune and Anders Sandholm (BRICS)</i>	
Demonstrations	
Formal System Development with KIV	363
<i>Michael Balser, Wolfgang Reif, Gerhard Schellhorn, Kurt Stenzel, and Andreas Thums (Universität Ulm)</i>	
More About TAS and IsaWin — Tools for Formal Program Development .	367
<i>Christoph Lüth (Universität Bremen) and Burkhart Wolff (Albert-Ludwigs-Universität Freiburg)</i>	
Using Maude	371
<i>Manuel Clavel (University of Navarre), Francisco Durán, Steven Eker, Patrick Lincoln (SRI), Narciso Martí-Oliet (Universidad Complutense, Madrid), Jose Meseguer (SRI), and Jose F. Quesada (CICA, Seville)</i>	
Author Index	375