

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Frank S. de Boer Marcello M. Bonsangue
Eric Madelaine (Eds.)

Formal Methods for Components and Objects

7th International Symposium, FMCO 2008
Sophia Antipolis, France, October 21-23, 2008
Revised Lectures



Springer

Volume Editors

Frank S. de Boer

Centre for Mathematics and Computer Science, CWI
Science Park 123, 1098 XG Amsterdam, The Netherlands
E-mail: F.S.de.Boer@cwi.nl

Marcello M. Bonsangue

Leiden Institute of Advanced Computer Science, Leiden University
P.O. Box 9512, 2300 RA Leiden, The Netherlands
E-mail: marcello@liacs.nl

Eric Madelaine

INRIA, Centre Sophia Antipolis
2004 route des Lucioles, B.P. 93, 06902 Sophia Antipolis, France
E-mail: eric.madelaine@sophia.inria.fr

Library of Congress Control Number: 2009933501

CR Subject Classification (1998): D.2, D.3, F.3, D.4, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743

ISBN-10 3-642-04166-3 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-04166-2 Springer 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. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12742981 06/3180 5 4 3 2 1 0

Preface

Large and complex software systems provide the necessary infrastructure in all industries today. In order to construct such large systems in a systematic manner, the focus in development methodologies has switched in the last two decades from functional issues to structural issues: both data and functions are encapsulated into software units which are integrated into large systems by means of various techniques supporting reusability and modifiability. This encapsulation principle is essential to both the object-oriented and the more recent component-based software engineering paradigms.

Formal methods have been applied successfully to the verification of medium-sized programs in protocol and hardware design. However, their application to the development of large systems requires more emphasis on specification, modeling and validation techniques supporting the concepts of reusability and modifiability, and their implementation in new extensions of existing programming languages like Java.

The 7th Symposium on Formal Methods for Components and Objects was held in Sophia Antipolis, France, during October 21–23, 2008. It was realized as a concertation meeting of European projects focussing on formal methods for components and objects. This volume contains the contributions submitted after the symposium by the speakers of each of the following European IST projects involved in the organization of the program:

- The IST-FP7 project COMPAS on compliance-driven models, languages, and architectures for services. The contact person is Schahram Dustdar (Technical University of Vienna, Austria)
- The IST-FP6 project CREDO on modelling and analysis of evolutionary structures for distributed services. The contact person is Frank de Boer (CWI, The Netherlands).
- The IST-FP7 DEPLOY on industrial deployment of advanced system engineering methods for high productivity and dependability. The contact person is Alexander Romanovsky (Newcastle University, UK).
- The IST-FP6 project GridComp on grid programming with components. The contact person is Denis Caromel (INRIA Sophia-Antipolis, France).
- The IST-FP6 project MOBIUS aiming at developing the technology for establishing trust and security for the next generation of global computers, using the proof carrying code paradigm. The contact person is Gilles Barthe (IMDEA Software, Spain).

The proceedings of the previous editions of FMCO have been published as volumes 2852, 3188, 3657, 4111, 4709 and 5382 of Springer’s *Lecture Notes in Computer Science*. We believe that these proceedings provide a unique combination of ideas on software engineering and formal methods which reflect the expanding body of knowledge on modern software systems.

Finally, we thank all authors for the high quality of their contributions, and the reviewers for their help in improving the papers for this volume.

June 2009

Frank de Boer
Marcello Bonsangue
Eric Madelaine

Organization

FMCO 2008 was part of the 5th Grids@Work event, co-organized by ERCIM, ETSI, INRIA, I3S, and CNRS. The 5th Grids@Work event was composed of:

The 5th Grid Plugtest, including the *Grids for Finance and Telecommunication Contest*

The GridCOMP conference

The FMCO symposium

The European technical concertation meeting *From Components to Services to Utilities* by the European units D3, *Software, Service Architectures and Infrastructures*, and F3, *eInfrastructures*

ProActive and GCM user groups and tutorials

The FMCO symposia are organized in the context of the project Mobi-J, a project founded by a bilateral research program of The Dutch Organization for Scientific Research (NWO) and the Central Public Funding Organization for Academic Research in Germany (DFG). The partners of the Mobi-J projects are: the Centrum voor Wiskunde en Informatica, the Leiden Institute of Advanced Computer Science, and the Christian-Albrechts-Universität Kiel.

This project aims at the development of a programming environment which supports component-based design and verification of Java programs annotated with assertions. The overall approach is based on an extension of the Java language with a notion of component that provides for the encapsulation of its internal processing of data and composition in a network by means of mobile asynchronous channels.

Sponsoring Institutions

The Dutch Organization for Scientific Research (NWO)

L’Institut National de Recherche en Informatique et Automatique (INRIA)

Le Laboratoire d’Informatique, Signaux et Systèmes de Sophia-Antipolis (I3S, Université de Nice Sophia-Antipolis et CNRS)

Table of Contents

The COMPAS Project

Reusable Architectural Decision Model for Model and Metadata Repositories	1
<i>Christine Mayr, Uwe Zdun, and Schahram Dustdar</i>	

Formal Behavioral Modeling and Compliance Analysis for Service-Oriented Systems	21
<i>Natallia Kokash and Farhad Arbab</i>	

The CREDO Project

A Real-Time Extension of Creol for Modelling Biomedical Sensors	42
<i>Marcel Kyas and Einar Broch Johnsen</i>	

Conformance Testing of Distributed Concurrent Systems with Executable Designs	61
<i>Bernhard K. Aichernig, Andreas Griesmayer, Einar Broch Johnsen, Rudolf Schlatte, and Andries Stam</i>	

Formal Verification for Components and Connectors	82
<i>Christel Baier, Tobias Blechmann, Joachim Klein, and Sascha Klüppelholz</i>	

The DEPLOY Project

Formal Modular Modelling of Context-Awareness	102
<i>Mats Neovius and Kaisa Sere</i>	

Towards Demonstrably Correct Compilation of Java Byte Code	119
<i>Michael Leuschel</i>	

Incremental System Modelling in Event-B	139
<i>Stefan Hallerstede</i>	

The GRIDCOMP Project

An Asynchronous Distributed Component Model and Its Semantics	159
<i>Ludovic Henrio, Florian Kammüller, and Marcela Rivera</i>	

Specification and Verification for Grid Component-Based Applications: From Models to Tools	180
<i>Antonio Cansado and Eric Madelaine</i>	

Semi-formal Models to Support Program Development: Autonomic Management within Component Based Parallel and Distributed Programming	204
<i>M. Aldinucci, M. Danelutto, and P. Kilpatrick</i>	
The MOBIUS Project	
Session-Based Compilation Framework for Multicore Programming	226
<i>Nobuko Yoshida, Vasco Vasconcelos, Hervé Paulino, and Kohei Honda</i>	
Abstract Interpretation of Symbolic Execution with Explicit State Updates	247
<i>Richard Bubel, Reiner Hähnle, and Benjamin Weiß</i>	
BML and Related Tools	278
<i>Jacek Chrząszcz, Marieke Huisman, and Aleksy Schubert</i>	
Author Index	299