

*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

*TU Dortmund University, 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 for Informatics, Saarbruecken, Germany*

Frank S. de Boer   Marcello M. Bonsangue  
Stefan Hallerstedte   Michael Leuschel (Eds.)

# Formal Methods for Components and Objects

8th International Symposium, FMCO 2009  
Eindhoven, The Netherlands, November 4-6, 2009  
Revised Selected Papers

## Volume Editors

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

Marcello M. Bonsangue  
Leiden University  
Leiden Institute of Advanced Computer Science  
Leiden, The Netherlands  
E-mail: marcello@liacs.nl

Stefan Hallerstede  
Heinrich-Heine University of Dusseldorf  
Department of Computer Science  
Dusseldorf, Germany  
E-mail: halstefa@cs.uni-duesseldorf.de

Michael Leuschel  
Heinrich-Heine University of Dusseldorf  
Department of Computer Science  
Dusseldorf, Germany  
E-mail: leuschel@cs.uni-duesseldorf.de

Library of Congress Control Number: 2010938608

CR Subject Classification (1998): D.2.4, D.2, D.3, F.3, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

|         |                                                       |
|---------|-------------------------------------------------------|
| ISSN    | 0302-9743                                             |
| ISBN-10 | 3-642-17070-6 Springer Berlin Heidelberg New York     |
| ISBN-13 | 978-3-642-17070-6 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 2010  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper 06/3180

# Preface

Large and complex software systems provide 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 that 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 8th Symposium on Formal Methods for Components and Objects was held in Eindhoven, The Netherlands, November 4–6, 2009. It was realized as a concertation meeting of European projects focusing on formal methods for components and objects. This volume contains 17 revised papers submitted after the symposium by the speakers of each of the following European IST projects involved in the organization of the program:

- IST-FP6 project BIONETS on biologically inspired services evolution for the pervasive age. The contact person for work relating to FMCO is Ludovic Henrio (INRIA Sophia-Antipolis, France).
- 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 modeling and analysis of evolutionary structures for distributed services. The contact person is Frank de Boer (CWI, The Netherlands).
- The IST-FP7 project 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-FP7 project HATS on highly adaptable and trustworthy software using formal methods. The contact person is Reiner Hähnle (Chalmers University of Technology, Sweden).
- The IST-FP7 project INESS on integrated European railway signaling system. The contact person for work relating to FMCO is Jim Woodcock (University of York, UK).
- The IST-FP7 project MOGENTES on model-based generation of tests for dependable embedded systems. The contact person for work relating to FMCO is Bernhard Aichernig (TU Graz, Austria).

- The IST-FP6 project PROTEST on property based testing. The contact person is John Derrick (University of Sheffield, UK).
- The IST-FP7 project QUASIMODO on quantitative system properties in model-driven design of embedded systems. The contact person is Kim G. Larsen (Aalborg University, Denmark).

We have also invited members of the working group on Formal Methods and Service-Oriented Architecture (FM-SOA) to participate.

The proceedings of the previous editions of FMCO have been published as volumes 2852, 3188, 3657, 4111, 4709, 5382, and 5751 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 2010

Frank de Boer  
 Marcello Bonsangue  
 Stefan Hallerstede  
 Michael Leuschel

# Organization

FMCO 2009 was part of the Formal Methods Week at Eindhoven, The Netherlands. Within the Formal Methods Week, the FMCO symposium was co-located with a host of conferences and workshops:

- The Symposium on Communicating Process Architectures (CPA)
- The International Workshop on Formal Aspects of Component Software (FACS)
- The Workshop on Formal Aspects of Security and Trust (FAST)
- The International Symposium on Formal Methods (FM)
- The International Workshop on Formal Methods for Industrial Critical Systems (FMICS)
- The International Workshop on Parallel and Distributed Methods in verification (PDMC)
- The 2009 Refine Workshop
- The 21st IFIP International Conference on Testing of Communicating Systems (TESTCOM)
- The 9th International Workshop on Formal Approaches to Testing of Software (FATES)
- The Dutch Testing Day
- The Second International FME Conference on Teaching Formal Methods (TFM)

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 the 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)

# Table of Contents

## The BIONETS Project

|                                                                   |   |
|-------------------------------------------------------------------|---|
| A Framework for Reasoning on Component Composition . . . . .      | 1 |
| <i>Ludovic Henrio, Florian Kammüller, and Muhammad Uzair Khan</i> |   |

## The COMPAS Project

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Verification of Context-Dependent Channel-Based Service Models . . . . . | 21 |
| <i>Natallia Kokash, Christian Krause, and Erik P. de Vink</i>            |    |

## The CREDO Project

|                                                                                                                                                                                                                                                                                                                                               |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| The Credo Methodology (Extended Version) . . . . .                                                                                                                                                                                                                                                                                            | 41 |
| <i>Immo Grabe, Mohammad Mahdi Jaghoori, Joachim Klein,<br/>Sascha Klüppelholz, Andries Stam, Christel Baier,<br/>Tobias Blechmann, Bernhard K. Aichernig, Frank de Boer,<br/>Andreas Griesmayer, Einar Broch Johnsen, Marcel Kyas,<br/>Wolfgang Leister, Rudolf Schlatte, Martin Steffen, Simon Tschirner,<br/>Liang Xuedong, and Wang Yi</i> |    |

## The DEPLOY Project

|                                                                                         |    |
|-----------------------------------------------------------------------------------------|----|
| Guided Formal Development: Patterns for Modelling and Refinement . . .                  | 70 |
| <i>Alexei Iliashov, Elena Troubitsyna, Linas Laibinis, and<br/>Alexander Romanovsky</i> |    |
| Applying Event-B Atomicity Decomposition to a Multi Media<br>Protocol . . . . .         | 89 |
| <i>Asieh Salehi Fathabadi and Michael Butler</i>                                        |    |

## The FM-SOA Working Group

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| Abstract Certification of Global Non-interference in Rewriting Logic . . . | 105 |
| <i>Mauricio Alba-Castro, María Alpuente, and Santiago Escobar</i>          |     |

## The HATS Project

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Interleaving Symbolic Execution and Partial Evaluation . . . . . | 125 |
| <i>Richard Bubel, Reiner Hähnle, and Ran Ji</i>                  |     |

## The INESS Project

|                                                                                          |     |
|------------------------------------------------------------------------------------------|-----|
| The Use of Model Transformation in the INESS Project .....                               | 147 |
| <i>Osmar M. dos Santos, Jim Woodcock, Richard F. Paige, and Steve King</i>               |     |
| Suitability of mCRL2 for Concurrent-System Design: A $2 \times 2$ Switch Case Study..... | 166 |
| <i>Frank P.M. Stappers, Michel A. Reniers, and Jan Friso Groote</i>                      |     |

## The MOGENTES Project

|                                                                                                                                 |     |
|---------------------------------------------------------------------------------------------------------------------------------|-----|
| Mapping UML to Labeled Transition Systems for Test-Case Generation: A Translation via Object-Oriented Action Systems .....      | 186 |
| <i>Willibald Krenn, Rupert Schlick, and Bernhard K. Aichernig</i>                                                               |     |
| Mutation-Based Test Case Generation for Simulink Models.....                                                                    | 208 |
| <i>Angelo Brillout, Nannan He, Michele Mazzucchi, Daniel Kroening, Mitra Purandare, Philipp Rümmer, and Georg Weissenbacher</i> |     |
| Model-Based Mutation Testing of Hybrid Systems.....                                                                             | 228 |
| <i>Bernhard K. Aichernig, Harald Brandl, Elisabeth Jöbstl, and Willibald Krenn</i>                                              |     |

## The PROTEST Project

|                                                                                                                                                             |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Property-Based Testing – The ProTest Project .....                                                                                                          | 250 |
| <i>John Derrick, Neil Walkinshaw, Thomas Arts, Clara Benac Earle, Francesco Cesarini, Lars-Ake Fredlund, Victor Gulias, John Hughes, and Simon Thompson</i> |     |
| Incrementally Discovering Testable Specifications from Program Executions .....                                                                             | 272 |
| <i>Neil Walkinshaw and John Derrick</i>                                                                                                                     |     |

## The QUASIMODO Project

|                                                                                      |     |
|--------------------------------------------------------------------------------------|-----|
| Methodologies for Specification of Real-Time Systems Using Timed I/O Automata.....   | 290 |
| <i>Alexandre David, Kim G. Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wąsowski</i> |     |
| The How and Why of Interactive Markov Chains.....                                    | 311 |
| <i>Holger Hermanns and Joost-Pieter Katoen</i>                                       |     |

|                           |            |
|---------------------------|------------|
| <b>Author Index .....</b> | <b>339</b> |
|---------------------------|------------|