

*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*

Farhad Arbab Peter Csaba Ölveczky (Eds.)

# Formal Aspects of Component Software

8th International Symposium, FACS 2011

Oslo, Norway, September 14-16, 2011

Revised Selected Papers



Springer

## Volume Editors

Farhad Arbab  
Centre for Mathematics  
and Computer Science (CWI)  
Science Park 123  
1098 XG Amsterdam, The Netherlands  
E-mail: farhad@cwi.nl

Peter Csaba Ölveczky  
University of Oslo  
Department of Informatics  
Postboks 1080 Blindern  
0316 Oslo, Norway  
E-mail: peterol@ifi.uio.no

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-35742-8 e-ISBN 978-3-642-35743-5  
DOI 10.1007/978-3-642-35743-5  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012954139

CR Subject Classification (1998): D.2.4, D.2, F.4, F.3, H.3.5, D.3, D.1, K.6.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

This volume contains the revised versions of accepted regular papers presented at the 8th International Symposium on Formal Aspects of Component Software (FACS 2011), held at the Department of Informatics, University of Oslo, on September 14–16, 2011. It also contains contributions by the three invited speakers at this event: José Meseguer, John Rushby, and Ketil Stølen.

FACS 2011 was the eighth event in a series founded by the International Institute for Software Technology of the United Nations University (UNU-IIST). The objective of FACS is to bring researchers and practitioners of component software and formal methods together in order to foster a deeper understanding of reliable component-based systems development and their applications, using formal methods. The component-based software development approach has emerged as a promising paradigm to cope with the complexity of present-day software systems by bringing sound engineering principles into software engineering. However, many challenging conceptual and technological issues still remain in the theory and practice of component-based software development. Moreover, the advent of service-oriented computing has brought to the fore new dimensions, such as quality of service and robustness to withstand inevitable faults, that require revisiting established component-based concepts in order to meet the new requirements of the service-oriented paradigm.

We received 46 submissions from 26 countries, out of which the Program Committee accepted 16 as regular papers, and, furthermore, conditionally accepted 4 additional papers. The revised versions of 18 of these papers appear in this volume. Each submission to FACS 2011 was reviewed by at least three referees.

Many colleagues and friends contributed to FACS 2011. First, we thank the authors who submitted their work to FACS 2011 and who, by their contributions and participation, made this symposium a high-quality event. We thank the Program Committee members and their sub-reviewers for their timely and insightful reviews as well as for their involvement in the post-reviewing discussions. We are also grateful to the FACS Steering Committee for its guidance, to the invited speakers, and to Lucian Bentea for all his assistance in organizing this event. Finally, we thank Andrei Voronkov for the excellent EasyChair conference system, and the Research Council of Norway and the Department of Informatics at the University of Oslo for financially supporting the symposium.

April 2012

Farhad Arbab  
Peter Ölveczky

# Organization

## Program Chairs

Farhad Arbab

Peter Csaba Ölveczky

CWI and Leiden University, The Netherlands

University of Oslo, Norway

## Steering Committee

Zhiming Liu (Coordinator)

Farhad Arbab

Luís Barbosa

Carlos Canal

Markus Lumpe

Eric Madelaine

Peter Csaba Ölveczky

Corina Păsăreanu

Bernhard Schätz

IIST UNU, Macau

CWI and Leiden University, The Netherlands

University of Minho, Portugal

University of Málaga, Spain

Swinburne University of Technology, Australia

INRIA, Centre Sophia Antipolis, France

University of Oslo, Norway

NASA Ames, USA

fortiss GmbH, Germany

## Program Committee

Erika Ábrahám

Farhad Arbab

Christel Baier

Luís Barbosa

Mihaela Bobaru

Christiano Braga

Roberto Bruni

Carlos Canal

Frank De Boer

Francisco Duran

Rolf Hennicker

RWTH Aachen University, Germany

CWI and Leiden University, The Netherlands

Technical University of Dresden, Germany

Universidade do Minho, Portugal

NASA/JPL, USA

Universidade Federal Fluminense, Brazil

University of Pisa, Italy

University of Málaga, Spain

CWI, The Netherlands

University of Málaga, Spain

Ludwig-Maximilians-Universität München,  
Germany

Alexander Knapp

Zhiming Liu

Markus Lumpe

Eric Madelaine

Sun Meng

Peter Csaba Ölveczky

Corina Păsăreanu

František Plášil

Augsburg University, Germany

IIST UNU, Macau

Swinburne University of Technology, Australia

INRIA, Centre Sophia Antipolis, France

Peking University, China

University of Oslo, Norway

NASA Ames, USA

Charles University, Czech Republic

Gwen Salaün  
Bernhard Schätz  
Wolfram Schulte  
Nishant Sinha  
Marjan Sirjani  
Volker Stolz  
Carolyn Talcott  
Emilio Tuosto

Grenoble INP - INRIA, France  
fortiss GmbH, Germany  
Microsoft Research, USA  
NEC Labs, Princeton, USA  
Reykjavik University, Iceland  
University of Oslo, Norway  
SRI International, USA  
University of Leicester, UK

## Additional Reviewers

Adam, Ludwig  
Ardourel, Gilles  
Bauer, Sebastian  
Baumeister, Hubert  
Bertolini, Cristiano  
Blech, Jan Olaf  
Chen, Zhenbang  
Choppy, Christine  
Corzilius, Florian  
Dan, Li  
Faber, Johannes  
Guancia, Roberto  
Helvensteijn, Michiel  
Henrio, Ludovic  
Hölzl, Florian  
Jaghori, Mohammad Mahdi  
Jansen, Nils  
Jezek, Pavel  
Jongmans, Sung  
Kemper, Stephanie  
Kezni, Jaroslav  
Khakpour, Narges  
Khalil, Maged

Khamespanah, Ehsan  
Khosravi, Ramtin  
Kofron, Jan  
Komuravelli, Anvesh  
Lang, Frédéric  
Lepri, Daniela  
Lluch Lafuente, Alberto  
Loup, Ulrich  
Malohlava, Michal  
Melgratti, Hernan  
Morisset, Charles  
Nellen, Johanna  
Ouederni, Meriem  
Pfaller, Christian  
Poch, Tomas  
Ramalho, Franklin  
Rodrigues, Genaina  
Sabouri, Hamideh  
Schlatte, Rudolf  
Schäf, Martin  
Verdejo, Alberto  
Vogler, Walter

# Table of Contents

Taming Distributed System Complexity through Formal Patterns . . . . .	1
<i>José Meseguer</i>	
Composing Safe Systems . . . . .	3
<i>John Rushby</i>	
A Denotational Model for Component-Based Risk Analysis . . . . .	12
<i>Gyrd Brændeland, Atle Refsdal, and Ketil Stølen</i>	
Synthesis of Hierarchical Systems . . . . .	42
<i>Benjamin Aminof, Fabio Mogavero, and Aniello Murano</i>	
A Modal Specification Theory for Components with Data . . . . .	61
<i>Sebastian S. Bauer, Kim Guldstrand Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wąsowski</i>	
Evaluating the Performance of Model Transformation Styles in Maude . . . . .	79
<i>Roberto Bruni and Alberto Lluch Lafuente</i>	
Interactive Transformations from Object-Oriented Models to Component-Based Models . . . . .	97
<i>Dan Li, Xiaoshan Li, Zhiming Liu, and Volker Stolz</i>	
Runtime Verification of Temporal Patterns for Dynamic Reconfigurations of Components . . . . .	115
<i>Julien Dormoy, Olga Kouchnarenko, and Arnaud Lanoix</i>	
Timed Conformance Testing for Orchestrated Service Discovery . . . . .	133
<i>Jose Pablo Escobedo, Christophe Gaston, and Pascale Le Gall</i>	
Realizability of Choreographies for Services Interacting Asynchronously . . . . .	151
<i>Gregor Gössler and Gwen Salaün</i>	
Networks of Real-Time Actors: Schedulability Analysis and Coordination . . . . .	168
<i>Mohammad Mahdi Jaghoori, Ólafur Hlynsson, and Marjan Sirjani</i>	
A Formal Model of Object Mobility in Resource-Restricted Deployment Scenarios . . . . .	187
<i>Einar Broch Johnsen, Rudolf Schlatte, and Silvia Lizeth Tapia Tarifa</i>	

The Logic of XACML .....	205
<i>Carroline Dewi Puspa Kencana Ramli, Hanne Riis Nielson, and Flemming Nielson</i>	
A Proof Assistant Based Formalization of MDE Components .....	223
<i>Mounira Kezadri, Benoît Combemale, Marc Pantel, and Xavier Thirion</i>	
Controlling an Iteration-Wise Coherence in Dataflow .....	241
<i>Sébastien Limet, Sophie Robert, and Ahmed Turki</i>	
Learning from Failures: A Lightweight Approach to Run-Time Behavioural Adaptation .....	259
<i>José Antonio Martín, Antonio Brogi, and Ernesto Pimentel</i>	
Verifying Safety of Fault-Tolerant Distributed Components .....	278
<i>Rabéa Ameur-Boulifa, Raluca Halalai, Ludovic Henrio, and Eric Madelaine</i>	
Reducing the Model Checking Cost of Product Lines Using Static Analysis Techniques .....	296
<i>Hamideh Sabouri and Ramtin Khosravi</i>	
Biographical Modelling of Architectural Patterns .....	313
<i>Alejandro Sanchez, Luís Soares Barbosa, and Daniel Riesco</i>	
Coordinated Execution of Heterogeneous Service-Oriented Components by Abstract State Machines .....	331
<i>Davide Brugali, Luca Gherardi, Elvinia Riccobene, and Patrizia Scandurra</i>	
Verifying Temporal Properties of Use-Cases in Natural Language .....	350
<i>Viliam Simko, David Hauzar, Tomas Bures, Petr Hnetynka, and Frantisek Plasil</i>	
<b>Author Index</b> .....	369