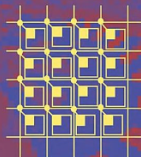


Bernhard K. Aichernig
Frank S. de Boer
Marcello M. Bonsangue (Eds.)

Formal Methods for Components and Objects

9th International Symposium, FMCO 2010
Graz, Austria, November/December 2010
Revised Papers



 Springer

Published in cooperation with

Lecture Notes in Computer Science

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

Bernhard K. Aichernig Frank S. de M
Marcello M. Bonsangue (Eds.)

Formal Methods for Component and Objects

9th International Symposium, FMCO
Graz, Austria, November 29 - December 1, 2007
Revised Papers

Volume Editors

Bernhard K. Aichernig
Graz University of Technology
Institute for Software Technology
Inffeldgasse 16b
8010 Graz, Austria
E-mail: aichernig@ist.tugraz.at

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-25270-9 e-ISSN 978-3-642-
DOI 10.1007/978-3-642-25271-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number:

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

Preface

Large and complex software systems provide the necessary infrastructure for many industries today. In order to construct such large systems in a reliable and efficient way, the focus in development methodologies has switched in the last decades from functional issues to structural issues: both data and functional components are decomposed into software units which are integrated into large systems using modular development techniques supporting reusability and modifiability. This emphasis on modularity is essential to both the object-oriented and the more recent component-oriented software engineering paradigms.

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

The 9th Symposium on Formal Methods for Components and Objects (FMCO 2010) was held in Graz, Austria, from November 29 to December 1, 2010. The venue was Hotel Weitzer. FMCO 2010 was realized as a co-located event with the 10th European project focussing on formal methods for components (FMC 2010). This volume contains 20 revised papers submitted after the symposium. The speakers of each of the following European projects involved in the program:

- The FP7-IST project AVANTSSAR on automated verification and security of service-oriented architectures. The contact person is Roberto Giacobazzi (University of Verona, Italy).
- The FP7-IST project DEPLOY on industrial deployment and engineering methods for high productivity and dependability. The contact person is Alexander Romanovsky (Newcastle University).

- The FP7-IST project MOGENTES on model-based guaranteed dependability of embedded systems. The contact person at FMCO is Bernhard Aichernig (Graz University of Technology, Austria).
- The FP7-IST project MULTIFORM on integrated multiplatform support for the design of networked embedded control systems. The contact person for work relating to FMCO is Christian Sonnenschein (University of Duisburg-Essen, Germany).
- The FP7-IST project QUASIMODO on quantitative model-driven design of embedded systems. The contact person is Larsen (Aalborg University, Denmark).

The proceedings of the previous editions of FMCO have been published in the *Lecture Notes in Computer Science* series, volumes 2852, 3188, 3657, 4111, 4709, 5382, 5751, and 6286. This volume is part of the *Notes in Computer Science*. We believe that these proceedings represent a valuable combination of ideas on software engineering and formal methods, and will contribute to the expanding body of knowledge on modern software systems.

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

July 2011

Bo

Organization

FMCO 2010 was organized by the Institute for Software Technology, University of Technology, Austria, in collaboration with the Centrum voor Informatica (CWI), Amsterdam, and the Leiden Institute of Computer Science, Leiden University, The Netherlands.

Program Organizer

Bernhard K. Aichernig Graz University of Technology

Steering Committee

Frank de Boer	CWI and Leiden University
Marcello Bonsangue	Leiden University, The Netherlands
Stefan Hallerstede	University of Düsseldorf, Germany
Michael Leuschel	University of Düsseldorf, Germany
Eric Madelaine	INRIA Méditerranée, France

Local Organization at Graz University of Technology

Bernhard K. Aichernig (Chair)
Harald Brandl
Arabella Gaß
Elisabeth Jöbstl
Petra Pichler
Herbert Pöckl
Stefan Tiran
Benedict Wright

Table of Contents

The AVANTSSAR Project

ASLan++ — A Formal Security Specification Language for Systems	
	<i>David von Oheimb and Sebastian Mödersheim</i>

Orchestration under Security Constraints	
	<i>Yannick Chevalier, Mohamed Anis Mekki, and Michaël</i>

Customizing Protocol Specifications for Detecting Resource and Guessing Attacks	
	<i>Bogdan Groza and Marius Minea</i>

The ESF Cost Action IC0701

Improving the Usability of Specification Languages and Model Annotation-Based Verification	
	<i>Bernhard Beckert, Thorsten Bormer, and Vladimir Kle</i>

Program Specialization via a Software Verification Tool ..	
	<i>Richard Bubel, Reiner Hähnle, and Ran Ji</i>

The DEPLOY Project

Model-Based Analysis Tools for Component Synthesis ...	
	<i>Luigia Petre, Kaisa Sere, and Leonidas Tsiopoulos</i>
Shared Event Composition/Decomposition in Event-B ...	
	<i>Renato Silva and Michael Butler</i>

The HATS Project

ABS: A Core Language for Abstract Behavioral Specifications

*Einar Broch Johnsen, Reiner Hähnle, Jan Schäfer,
Rudolf Schlatte, and Martin Steffen*

A Component Model for the ABS Language

*Michaël Lienhardt, Ivan Lanese, Mario Bravetti, David
Gianluigi Zavattaro, Yannick Welsch, Jan Schäfer, and
Arnd Poetzsch-Heffter*