Lecture Notes in Computer Science 4789

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

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
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Michael Butler Michael G. Hinchey
María M. Larrondo-Petrie (Eds.)

Formal Methods and Software Engineering

9th International Conference
on Formal Engineering Methods, ICFEM 2007
Boca Raton, FL, USA, November 14-15, 2007
Proceedings

Springer

Volume Editors

Michael Butler
University of Southampton, School of Electronic and Computer Science
Highfield, Southampton, SO17 1BJ, UK
E-mail: m.j.butler@ecs.soton.ac.uk

Michael G. Hinchey
Loyola College in Maryland, Department of Computer Science
4501 N. Charles Street, Baltimore, MD 21210, USA
E-mail: mike.hinchey@usa.net

María M. Larrondo-Petrie
Florida Atlantic University, Department of Computer Science and Engineering
777 Glades Road SE-308, Boca Raton, FL 33431-0991, USA
E-mail: petrie@fau.edu

Library of Congress Control Number: 2007938401

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-76648-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-76648-3 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12187614 06/3180 5 4 3 2 1 0

Preface

Formal methods for the development of computer systems have been extensively researched and studied. A range of semantic theories, specification languages, design techniques, and verification methods and tools have been developed and applied to the construction of programs of moderate size that are used in critical applications. The challenge now is to scale up formal methods and integrate them into engineering development processes for the correct construction and maintenance of computer systems. This requires us to improve the state of the art by researching the integration of methods and their theories, and merging them into industrial engineering practice, including new and emerging practice.

ICFEM, the International Conference on Formal Engineering Methods, aims to bring together those interested in the application of formal engineering methods to computer systems. Researchers and practitioners, from industry, academia, and government, are encouraged to attend and to help advance the state of the art. The conference particularly encourages research that aims at a combination of conceptual and methodological aspects with their formal foundation and tool support, and work that has been incorporated into the production of real systems.

This volume contains the papers presented at ICFEM 2007 held November 14–15, 2007 in Florida Atlantic University, Boca Raton, Florida. There were 38 submissions. Each submission was reviewed by four Program Committee members. The committee decided to accept 19 papers based on originality, technical soundness, presentation, and relevance to formal engineering and verification methods. We thank the Program Committee members and the other referees for their effort and professional work in the reviewing and selecting process. The program also includes contributions from the two keynote speakers: Jean-Raymond Abrial and Tom Maibaum. Professor Abrial gave a talk on a system development process with Event-B and the Rodin Platform while Professor Maibaum gave a talk on the challenges of software certification.

A workshop on the *verifiable file store mini-challenge* was held on November 13, 2007 co-located with ICFEM 2007. This workshop was organized by Jim Woodcock and Leo Freitas as part of the Grand Challenge in Verified Software.

ICFEM 2007 was jointly organized and sponsored by Florida Atlantic University, Loyola College in Maryland, and the University of Southampton and we would like to thank all those who helped in the organization. We used the Easychair system to manage the submissions, refereeing, paper selection, and proceedings production. We would like to thank the Easychair team for a very powerful tool.

August 2007

Michael Butler
Mike Hinchey
Maria M. Larrondo-Petrie

Conference Organization

Conference Chair

General Chair	Mike Hinchey (Loyola College in Maryland, USA)
Program Chairs	Michael Butler (University of Southampton, UK)
	Maria M. Larrondo-Petrie (Florida Atlantic University, USA)
Publicity Chair	Denis Gracanin (Virginia Tech, USA)

Program Committee

Keijiro Araki
Farhad Arbab
David Basin
Ana Cavalcanti
Jessica Chen
Yoonsik Cheon
Kai Engelhardt
Eduardo B. Fernandez
Colin Fidge
John Fitzgerald
Marc Frappier
Marcelo Fabián Frias
Uwe Glässer
Joseph Kiniry
Shriram Krishnamurthi
Kung-Kiu Lau
Rustan Leino
Michael Leuschel
Xuandong Li
Zhiming Liu
Shaoying Liu
Tiziana Margaria
Huaikou Miao
Peter O'Hearn
Michael Poppleton
Marie-Laure Potet
Anders Ravn
Davide Sangiorgi
Mannu Satpathy
Klaus-Dieter Schewe
Kaisa Sere
Wuwei Shen
Marjan Sirjani
Ketil Stølen
Sofiene Tahar
Helen Treharne
T.H. Tse
Farn Wang
Wang Yi
Jian Zhang
Jin Song Dong
Zhenhua Duan

Local Organization

Eduardo B. Fernandez
Michael VanHilst
Nelly Delessy-Gassant
Maureen Manoly
Colleen Glazer

External Reviewers

Rezine Ahmed
Bernhard Aichernig
Joachim Baran
Achim D. Brucker
Neil Evans
Bernd Fischer
Wan Fokkink
Amjad Gawanmeh
Olga Grinchintein
Osman Hasan
Felix Klaedtke
István Knoll

Linas Laibinis
Yuan Fang Li
Sotiris Moschoyiannis
Juan Antonio Navarro-Pérez
Joseph Okika
Gennaro Parlato
Daniel Plagge
Marta Plaska
Sampath Prahlad
Zongyan Qiu
S. Ramesh
Niloofar Razavi
Atle Refsdal
Ragnhild Kobro Runde
Mehrnoosh Sadrzadeh
Mayank Saksena
Corinna Spermann
Volker Stolz
Jan Stöcker
Jun Sun
Leonidas Tsiopoulos
Andrzej Wasowski
Mohamed Zaki
Miaomiao Zhang
Jianhua Zhao
Hui Liang

ICFEM Steering Committee

He Jifeng (East China Normal University, China)
Keijiro Araki (Kyushu University, Japan)
Jin Song Dong (National University, Singapore)
Chris George (UNU-IIST, Macao)
Mike Hinchey (Loyola College in Maryland, USA)
Shaoying Liu (Hosei University, Japan)
John McDermid (University of York, UK)
Tetsuo Tamai (University of Tokyo, Japan)
Jim Woodcock (University of York, UK)

Table of Contents

Invited Talks

A System Development Process with Event-B and the Rodin Platform 1
Jean-Raymond Abrial

Challenges in Software Certification 4
Tom Maibaum

Security and Knowledge

Integrating Formal Methods with System Management 19
Martin de Groot

Formal Engineering of XACML Access Control Policies in VDM++ 37
Jeremy W. Bryans and John S. Fitzgerald

A Verification Framework for Agent Knowledge 57
Jin Song Dong, Yuzhang Feng, and Ho-fung Leung

Embedded Systems

From Model-Based Design to Formal Verification of Adaptive Embedded Systems 76
Rasmus Adler, Ina Schaefer, Tobias Schuele, and Eric Vecchié

Machine-Assisted Proof Support for Validation Beyond Simulink 96
Chunqing Chen, Jin Song Dong, and Jun Sun

VeSTA: A Tool to Verify the Correct Integration of a Component in a Composite Timed System 116
Jacques Julliand, Hassan Mountassir, and Emilie Oudot

Testing

Integrating Specification-Based Review and Testing for Detecting Errors in Programs 136
Shaoying Liu

Testing for Refinement in CSP 151
Ana Cavalcanti and Marie-Claude Gaudel

Reducing Test Sequence Length Using Invertible Sequences 171
Lihua Duan and Jessica Chen

Automated Analysis

Model Checking with SAT-Based Characterization of ACTL Formulas 191
Wenhui Zhang

Automating Refinement Checking in Probabilistic System Design 212
Carlos Gonzalia and Annabelle McIver

Model Checking in Practice: Analysis of Generic Bootloader Using SPIN 232
Kuntal Das Barman and Debapriyay Mukhopadhyay

Model Checking Propositional Projection Temporal Logic Based on SPIN 246
Cong Tian and Zhenhua Duan

Hardware

A Denotational Semantics for Handel-C Hardware Compilation 266
Juan Ignacio Perna and Jim Woodcock

Automatic Generation of Verified Concurrent Hardware 286
Marcel Oliveira and Jim Woodcock

Modeling and Verification of Master/Slave Clock Synchronization Using Hybrid Automata and Model-Checking 307
Guillermo Rodriguez-Navas, Julián Proenza, and Hans Hansson

Concurrency

Efficient Symbolic Execution of Large Quantifications in a Process Algebra 327
Benoît Fraikin and Marc Frappier

Formalizing SANE Virtual Processor in Thread Algebra 345
Thuy Duong Vu and Chris Jesshope

Calculating and Composing Progress Properties in Terms of the Leads-to Relation 366
Arjan J. Mooij

Erratum

Challenges in Software Certification E1
Tom Maibaum

Author Index 387