

Lecture Notes in Computer Science  
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2884

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Elie Najm Uwe Nestmann  
Perdita Stevens (Eds.)

# Formal Methods for Open Object-Based Distributed Systems

6th IFIP WG 6.1 International Conference, FMOODS 2003  
Paris, France, November 19-21, 2003  
Proceedings



Springer

## Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

## Volume Editors

Elie Najm  
ENST, Dépt. Informatique et Réseaux  
46, rue Barrault, 75634 Paris, France  
E-mail: Elie.Najm@enst.fr

Uwe Nestmann  
EPFL-I and C  
Ecublens INR 317, 1015 Lausanne, Switzerland  
E-mail: uwe.nestmann@EPFL.ch

Perdita Stevens  
University of Edinburgh, Laboratory for Foundations of Computer Science  
JCMB, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, UK  
E-mail: perdita.stevens@ed.ac.uk

## Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek  
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;  
detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): C.2.4, D.1.3, D.2, D.3, F.3, D.4

ISSN 0302-9743

ISBN 3-540-20491-1 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media GmbH  
[springeronline.com](http://springeronline.com)

© 2003 IFIP International Federation for Information Processing, Hofstrasse 3, A-2361 Laxenburg, Austria  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik  
Printed on acid-free paper SPIN: 10967973 06/3142 5 4 3 2 1 0

# Preface

This volume contains the proceedings of FMOODS 2003, the 6th IFIP WG 6.1 International Conference on *Formal Methods for Open Object-Based Distributed Systems*. The conference was held in Paris, France on November 19–21, 2003. The event was the sixth meeting of this conference series, which is held roughly every year and a half, the earlier events having been held in Paris, Canterbury, Florence, Stanford, and Twente.

The goal of the FMOODS series of conferences is to bring together researchers whose work encompasses three important and related fields:

- formal methods;
- distributed systems;
- object-based technology.

Such a convergence is representative of recent advances in the field of distributed systems, and provides links between several scientific and technological communities, as represented by the conferences FORTE/PSTV, CONCUR, and ECOOP.

The objective of FMOODS is to provide an integrated forum for the presentation of research in the above-mentioned fields, and the exchange of ideas and experiences in the topics concerned with the formal methods support for open object-based distributed systems. For the call for papers, aspects of interest of the considered systems included, but were not limited to: formal models; formal techniques for specification, design or analysis; component-based design; verification, testing and validation; semantics of programming, coordination, or modeling languages; type systems for programming, coordination or modelling languages; behavioral typing; multiple viewpoint modelling and consistency between different models; transformations of models; integration of quality of service requirements into formal models; formal models for security; and applications and experience, carefully described. Work on these aspects of (official and de facto) standard notations and languages, e.g., the UML, and on component-based design, was explicitly welcome.

In total 78 abstracts and 63 papers were submitted to this year's conference, covering the full range of topics listed above. Out of the submissions, 18 research papers were selected by the program committee for presentation. We would like to express our deepest appreciation to the authors of all submitted papers and to the program committee members and external reviewers who did an outstanding job in selecting the best papers for presentation.

For the first time, the FMOODS conference was held as a joint event in federation with the 4th IFIP WG 6.1 International Conference on *Distributed Applications and Interoperable Systems* (DAIS 2003). The co-location of the 2003 vintages of the FMOODS and DAIS conferences provided an excellent opportunity to the participants for a wide and comprehensive exchange of ideas within

the domain of distributed systems and applications. Both FMOODS and DAIS address this domain, the former with its emphasis on formal approaches, the latter on practical solutions. Their combination in a single event ensured that both theoretical foundations and practical issues were presented and discussed. Also due to the federation of the two conferences, the topics of reconfigurability and component-based design were particularly emphasized this year, along with the many open issues related to openness and interoperability of distributed systems and applications. To further the interaction between the two communities, participants to the federated event were offered a single registration procedure and were entitled to choose freely between DAIS and FMOODS sessions. Also, several invited speakers were explicitly scheduled as joint sessions. As another novelty, this year's conference included a two-day tutorial and workshop session, the latter again explicitly held as a joint event. Details can be found at the conference website: <http://fedconf.enst.fr/>.

Special thanks to Michel Riguidel, head of the Networks and Computer Science department of ENST. His support made this event happen. We would also like to thank Lynne Blair who chaired the workshop selection process, and Sylvie Vignes who chaired the tutorial selection process. We are grateful to David Chambliss, Andrew Herbert, Bart Jacobs, Bertrand Meyer, and Alan Cameron Wills for agreeing to present invited talks at the conference.

We thank Jennifer Tenzer for help with running the electronic submission and conference management system, and the Laboratory for Foundations of Computer Science at the University of Edinburgh for financially supporting this help. We used CyberChair (<http://www.cyberchair.org>); we thank Julian Bradfield for advice on adapting it for our particular needs. As of today, we have also received sponsorships from CNRS-ARP, GET, EDF, ENST, and INRIA. Other contributors are also expected. We extend our thanks to all of them.

We thank Laurent Pautet for acting as Local Arrangements Chair and John Derrick for his work as Publicity Chair. We would also like to thank the FMOODS Steering Committee members for their advice.

September 2003

Elie Najm  
FMOODS 2003 General Chair  
Uwe Nestmann  
Perdita Stevens  
FMOODS 2003 Program Chairs

# Organization

General Chair	Elie Najm (ENST, France)
Program Chairs	Uwe Nestmann (EPFL, Switzerland) Perdita Stevens (University of Edinburgh, UK)
Tutorial Chair	Sylvie Vignes (ENST, France)
Workshop Chair	Lynne Blair (Lancaster University, UK)
Local Organization Chair	Laurent Pautet (ENST, France)
Publicity Chair	John Derrick (University of Kent, UK)

## Steering Committee

John Derrick  
Roberto Gorrieri  
Guy Leduc  
Elie Najm

## Program Committee

Lynne Blair (UK)  
Michele Bugliesi (Italy)  
Denis Caromel (France)  
John Derrick (UK)  
Alessandro Fantechi (Italy)  
Kokichi Futatsugi (Japan)  
Andy Gordon (UK)  
Cosimo Laneve (Italy)  
Luigi Logrippo (Canada)  
Elie Najm (France)  
Erik Poll (The Netherlands)  
Arend Rensink (The Netherlands)  
Bernhard Rumpe (Germany)  
Martin Steffen (Germany)  
Carolyn Talcott (USA)  
Nalini Venkatasubramanian (USA)

## Referees

Erika Ábrahám  
Dave Akehurst  
Isabelle Attali  
Arnaud Bailly  
Paolo Baldan  
Tomás Barros  
Benoit Baudry  
Clara Benac Earle  
Nick Benton  
Kirill Bogdanov  
Tommaso Bolognesi  
Rabea Boulifa  
Julian Bradfield  
Sebastien Briaïs  
M. C. Bujorianu  
Daniel C. Bünzli  
Nadia Busi  
Arnaud Contes  
Steve Cook  
Grit Denker  
Vijay D'silva  
Juan Guillen Scholten  
Sebastian Gutierrez-Nolasco  
Ludovic Henrio  
Jozef Hooman  
Fabrice Huet  
Ralf Huuck  
Bart Jacobs  
Ferhat Khendek  
Juliana Küster Filipe  
Marcel Kyas

Giuseppe Lami  
Diego Latella  
Giuseppe Lipari  
Luigi Liquori  
Felipe Luna  
Eric Madelaine  
Ian Mason  
Mieke Massink  
Nikolay Mihaylov  
Shivajit Mohapatra  
Rocco Moretti  
Kazuki Munakata  
Masaki Nakamura  
Masahiro Nakano  
Kazuhiro Ogata  
Martijn Oostdijk  
Carla Piazza  
Fabio Pittarello  
Alberto Pravato  
Antonio Ravara  
Bernhard Reus  
Ant Rowstron  
Takahiro Seino  
Don Syme  
Alexandre Tauveron  
Jennifer Tenzer  
Lucian Wischik  
Jianwen Xiang  
Gianluigi Zavattaro  
Matthias Zenger



# Table of Contents

## Invited Talk

Java’s Integral Types in PVS .....	1
<i>Bart Jacobs</i>	

## Models

Towards Object-Oriented Graphs and Grammars .....	16
<i>Ana Paula Lüdtke Ferreira and Leila Ribeiro</i>	
A Rewriting Based Model for Probabilistic Distributed Object Systems ...	32
<i>Nirman Kumar, Koushik Sen, José Meseguer, and Gul Agha</i>	
Engineering the SDL Formal Language Definition .....	47
<i>Andreas Prinz and Martin v. Löwis</i>	

## Logic and Verification

A Syntax-Directed Hoare Logic for Object-Oriented Programming Concepts .....	64
<i>Cees Pierik and Frank S. de Boer</i>	
Inheritance of Temporal Logic Properties .....	79
<i>Heike Wehrheim</i>	
Temporal Logic Based Static Analysis for Non-uniform Behaviours .....	94
<i>Matthias Colin, Xavier Thirioux, and Marc Pantel</i>	

## Calculi

The Kell Calculus: Operational Semantics and Type System .....	109
<i>Philippe Bidingier and Jean-Bernard Stefani</i>	
A Calculus for Long-Running Transactions .....	124
<i>Laura Bocchi, Cosimo Laneve, and Gianluigi Zavattaro</i>	
Formal Analysis of Some Timed Security Properties in Wireless Protocols .....	139
<i>Roberto Gorrieri, Fabio Martinelli, Marinella Petrocchi, and Anna Vaccarelli</i>	

## Java and .NET

Inductive Proof Outlines for Monitors in Java . . . . .	155
<i>Erika Ábrahám, Frank S. de Boer, Willem-Paul de Roever, and Martin Steffen</i>	
Proof Scores in the OTS/CafeOBJ Method . . . . .	170
<i>Kazuhiro Ogata and Kokichi Futatsugi</i>	
Managing the Evolution of .NET Programs . . . . .	185
<i>Susan Eisenbach, Vladimir Jurisic, and Chris Sadler</i>	

## UML

On Mobility Extensions of UML Statecharts. A Pragmatic Approach . . . . .	199
<i>Diego Latella and Mieke Massink</i>	
New Operators for the TURTLE Real-Time UML Profile . . . . .	214
<i>Christophe Lohr, Ludovic Apvrille, Pierre de Saqui-Sannes, and Jean-Pierre Courtiat</i>	
Checking Consistency in UML Diagrams: Classes and State Machines . . . . .	229
<i>Holger Rasch and Heike Wehrheim</i>	

## Composition and Verification

Compositional Verification Using CADP of the ScalAgent Deployment Protocol for Software Components . . . . .	244
<i>Frédéric Tronel, Frédéric Lang, and Hubert Garavel</i>	
Verification of Distributed Object-Based Systems . . . . .	261
<i>Fernando L. Dotti, Luciana Foss, Leila Ribeiro, and Osmar M. dos Santos</i>	
Design and Verification of Distributed Multi-media Systems . . . . .	276
<i>David Akehurst, John Derrick, and A. Gill Waters</i>	

<b>Author Index</b> . . . . .	293
-------------------------------	-----