

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

1641

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Dieter Hutter Werner Stephan
Paolo Traverso Markus Ullmann (Eds.)

Applied Formal Methods – FM-Trends 98

International Workshop on Current Trends
in Applied Formal Methods
Boppard, Germany, October 7-9, 1998
Proceedings



Springer

Series Editors

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

Volume Editors

Dieter Hutter
Werner Stephan
German Research Center for Artificial Intelligence (DFKI GmbH)
Stuhlsatzenhausweg 3, D-66123 Saarbrücken, Germany
E-mail: {hutter/stephan}@dfki.de

Paolo Traverso
ITC-irst, Centro per la ricerca scientifica e tecnologica
via Sommarive, 18, I-38050 Povo (Trento), Italy
E-mail: leaf@itc.it

Markus Ullmann
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 183, D-53175 Bonn, Germany
E-mail: ullmann@bsi.de

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Applied formal methods - FM trends 98 : proceedings /
International Workshop on Current Trends in Applied Formal
Methods, Boppard, Germany, October 7 - 9, 1998. Dieter Hutter ...
(ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ;
London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1641)
ISBN 3-540-66462-9

CR Subject Classification (1998): F.3, D.2, D.1, D.3, I.2, F.4.1

ISSN 0302-9743

ISBN 3-540-66462-9 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 Berlin Heidelberg 1999
Printed in Germany

Typesetting: Camera-ready by author
SPIN: 10703472 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the contributions presented at the *International Workshop on Current Trends in Applied Formal Methods* organized October 7-9, 1998, in Boppard, Germany.

The main objective of the workshop was to draw a map of the key issues facing the practical application of formal methods in industry. This appears to be particularly timely with safety and security issues becoming a real obstacle to industrial software and hardware development. As a consequence, almost all major companies have now set up departments or groups to work with formal methods and many European countries face a severe labour shortage in this new field. Tony Hoare's prediction of the art of software (and hardware) development becoming a proper engineering science with its own body of tools and techniques is now becoming a reality.

So the focus of this application oriented workshop was not so much on special academic topics but rather on the many practical aspects of this emerging new technology: verification and validation, and tool support and integration into the software life-cycle. By evaluating the state of the art with respect to industrial applications a discussion emerged among scientists, practising engineers, and members of regulatory and funding agencies about future needs and developments. This discussion lead to roadmaps with respect to the future of this field, to tool support, and potential application areas and promising market segments. The contributions of the participants from industry as well as from the respective national security bureaus were particularly valuable and highly appreciated.

The workshop program included four invited talks, 16 talks selected by the program committee, and six talks given during the application day. Apart from the regular papers, the proceedings contain two invited contributions by Egon Börger and Manfred Broy, three application papers, and eight tool papers.

Egon Börger gives a new comprehensive introduction to Abstract State Machines describing their use in the different design stages of software systems. Manfred Broy and Oscar Slotosch present a process model for the integration of formal methods into conventional software engineering. They discuss the mediating role of user-oriented description techniques. Contributions presented at the application day cover industrial applications of model-checking (an excellent survey of current industrial practice was presented in the invited talk by Wolfram Büttner, SIEMENS), hardware-design (paper by Masahiro Fujita, Sree P. Rajan, and Alan Hu), safety critical control systems (paper by Meine van der Meulen and Tim Clement), and security engineering (paper by Frank Koob, Markus Ullmann, and Stefan Wittmann, BSI). The tool papers provide a collection of the major current systems.

Welcome Note

I welcome you cordially on behalf of the Federal Minister of the Interior and the Federal IT Security Agency at this international workshop, and I extend a special welcome to the many foreign guests and the invited speakers of the conference.

To look into the future and identify technological trends is a challenge that raises many questions. If one considers IT development in general, one comes to the conclusion that it is not unusual to talk about and handle technologies that have existed for fewer than 5 years now. Java and the World Wide Web are two illustrative examples. Their development and distribution is taking place at a breathtaking speed. I do not think that anybody would have predicted that these phenomena would take on such dimensions.

At the moment, technical systems in a wide range of fields are becoming ever more complex. Computer failures (breaking of access codes, T-online) and accidents (plane crashes, train disasters) arouse a latent feeling in society that technical systems are no longer fully controllable. The impression arises that against this background security will increasingly have to be discussed in its entirety, and that new promising procedures will have to be applied. We expect that it will be possible to achieve major improvements in terms of quality and security through *Formal Methods* (FM) in the field of software and hardware systems.

Yet new technologies alone are not enough. Those who make the laws must take action, too, in order to ensure that the technologies promising a higher level of security are used appropriately, and are not sacrificed for short-term economic profit. A high-level information technical security infrastructure is essential to ensure confidence in the flow of information on the data highways and acceptance of new technologies in politics, the economy, and society. The Digital Signature Act and Ordinance as well as the related detailed technical specifications have now created a basis in Germany for the development of a uniform security infrastructure. The high certification level of the components to be used means that the use of FM for digital signature components that comply with the law is mandatory.

The aim of the workshop, which starts today here at the Federal Academy, is, on the one hand, to provide information about current developments of IT, and to discuss and possibly orientate them towards the requirements of industry. On the other hand, you will exchange experience regarding the use of FM during the Application Day and thus encourage industrial companies to use FM in order to make a contribution to increasing security and safety.

I wish the workshop the best of success, which I combine with the hope that the workshop will give a clear signal for a wider applicability of formal methods.

October 1998

MinR Norbert Vogt
German Federal Ministry of the Interior

Workshop Organization

The *International Workshop on Current Trends in Applied formal Methods* (FM-Trends 98) was organized jointly by the DFKI GmbH (Deutsches Forschungszentrum für Künstliche Intelligenz, Saarbrücken), the BSI (Bundesamt für Sicherheit in der Informationstechnik, Bonn), the JRC (Joint Research Centre of the European Commission, Ispra) and the IRST (Istituto per la Ricerca Scientifica e Tecnologica, Trento).

Workshop Committee

F. Giunchiglia (Trento)	P. Traverso (Trento)
D. Hutter (Saarbrücken)	M. Ullmann (Bonn)
F. Koob (Bonn)	H.P. Wagner (Bonn)
J.H. Siekmann (Saarbrücken)	M. Wilikens (Ispra)
W. Stephan (Saarbrücken)	

Advisory Board

E. Astesiano, (Genova)	D. Harel, (Rehovot, Israel)
K.R. Apt, (Amsterdam)	T. Henzinger, (Berkeley)
J. Bergstra, (Amsterdam)	M. Hinchey, (New Jersey)
V. Berzins, (Monterey)	C.A.R. Hoare, (Oxford)
D. Bjorner, (Lyngby, Denmark)	D. Howe, (Bell Labs, USA)
R. Bloomfield, (Adelard)	N. Jones, (Copenhagen)
J. Bowen, (Berkshire)	D. Kapur, (New York)
B. Boyer, (Texas)	H. Kirchner, (Rocquencourt, France)
M. Broy, (Munich)	H. Langmaack, (Kiel)
A. Bundy, (Edinburgh)	T. Maibaum, (London)
E. Clarke, (CMU, USA)	U. Martin, (St. Andrews)
W. Damm, (Oldenburg)	U. Montanari, (Pisa)
J.W. de Bakker, (Amsterdam)	J S. Moore, (Texas)
W.P. de Roever, (Kiel)	T. Nipkow, (Munich)
H.D. Ehrich, (Braunschweig)	D. Parnas, (Hamilton)
E.A. Emerson, (Texas)	L. Paulson, (Cambridge)
H. Ganzinger, (Saarbrücken)	A. Ravn, (Lyngby, Denmark)
M.C. Gaudel, (Paris)	A. W. Roscoe, (Oxford)
J. Goguen, (Monterey)	J. Sifakis, (Paris)
D. Gries, (Ithaca, New York)	
Y. Gurevich, (Michigan)	

External Referees

Massimo Benerecetti
Piergiorgio Bertoli
Alessandro Cimatti
Marco Daniele

Dominique Mery
Olaf Müller
Marco Roveri
Roberto Sebastiani

Oscar Slotosch
Adolfo Villafiorita

Acknowledgements

All submitted papers were refereed by advisory board members, workshop organizers, and external referees. This workshop would not have been possible without their voluntary and dedicated work.

Table of Contents

Invited Papers

High Level System Design and Analysis Using Abstract State Machines . . .	1
<i>Egon Börger</i>	
Enriching the Software Development Process by Formal Methods	44
<i>Manfred Broy, Oscar Slotosch</i>	

Regular Papers

Formal Program Development in Geometric Modeling	62
<i>François Puitg, Jean-François Dufourd</i>	
Design of Distributed Multimedia Applications (DAMD)	77
<i>Wanderley Lopes de Souza, Paulo Nazareno Maia Sampaio, Jean-Marie Farines, Roberto Milton Scheffel, Maria Janilce B. Almeida, Luciano Paschoal Gaspary, Lissandro Zambenodetti Granville, Roberto Willrich, Murilo S. de Camargo, Marcelo Domingos</i>	
Structured Formal Verification of a Fragment of the IBM S/390 Clock Chip	92
<i>Alfons Geser, Wolfgang Kuchlin</i>	
Automated Test Set Generation for Statecharts	107
<i>K. Bogdanov, M. Holcombe, H. Singh</i>	
Rigorous Compiler Implementation Correctness: How to Prove the Real Thing Correct	122
<i>Wolfgang Goerigk, Ulrich Hoffmann</i>	
Translation Validation: From DC+ to C	137
<i>A. Pnueli, O. Shtrichman, M. Siegel</i>	
A Practical Hierarchical Design by Timed Simulation Relations for Real-Time Systems	151
<i>Satoshi Yamane</i>	
A Lightweight Approach to Formal Methods	168
<i>Sten Agerholm, Peter Gorm Larsen</i>	
An Open Environment for the Integration of Heterogeneous Modelling Techniques and Tools	184
<i>Robert Büssow, Wolfgang Grieskamp, Winfried Heicking, Stephan Herrmann</i>	

Integrating Domain Specific Language Design in the Software Life Cycle .	196
<i>Philipp W. Kutter, Daniel Schweizer, Lothar Thiele</i>	
Flexible and Reliable Process Model Properties: An Integrated Approach .	213
<i>Tiziana Margaria, Volker Gruhn</i>	
A Symbolic Model Checker for ACTL	228
<i>A. Fantechi, S. Gnesi, F. Mazzanti, R. Pugliese, E. Tronci</i>	
Critical Systems Validation and Verification with CSP and FDR	243
<i>Michael Goldsmith, Irfan Zakiuddin</i>	
UniForM Perspectives for Formal Methods	251
<i>Bernd Krieg-Brückner</i>	
The UniForM WorkBench - A Higher Order Tool Integration Framework .	266
<i>Einar W. Karlsen</i>	

Application Papers

Two Real Formal Verification Experiences: ATM Switch Chip and Parallel Cache Protocol	281
<i>Masahiro Fujita, Sree P. Rajan, Alan Hu</i>	
Formal Methods in the Specification of the Emergency Closing System of the Eastern Scheldt Storm Surge Barrier	296
<i>Meine van der Meulen, Tim Clement</i>	
The New Topicality of Using Formal Models of Security Policy within the Security Engineering Process	302
<i>Frank Koob, Markus Ullmann, Stefan Wittmann</i>	

Tool Papers

Towards Comprehensive Tool Support for Abstract State Machines: The ASM Workbench Tool Environment and Architecture	311
<i>Giuseppe Del Castillo</i>	
The IFAD VDM Tools: Lightweight Formal Methods	326
<i>Sten Agerholm, Peter Gorm Larsen</i>	
KIV 3.0 for Provably Correct Systems	330
<i>Michael Balser, Wolfgang Reif, Gerhard Schellhorn, Kurt Stenzel</i>	
PVS: An Experience Report	338
<i>S. Owre, J. M. Rushby, N. Shankar, and D. W. J. Stringer-Calvert</i>	
QUEST: Overview over the Project	346
<i>Oscar Slotosch</i>	

VSE: Controlling the Complexity in Formal Software Developments	351
<i>Dieter Hutter, Heiko Mantel, Georg Rock, Werner Stephan, Andreas Wolpers, Michael Balser, Wolfgang Reif, Gerhard Schellhorn, Kurt Stenzel</i>	
The wHOLe System	359
<i>Mark E. Woodcock</i>	
Z/EVES Version 1.5: An Overview	367
<i>ORA Canada</i>	
Author Index	377