

Lecture Notes in Computer Science

863

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

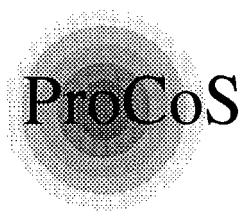
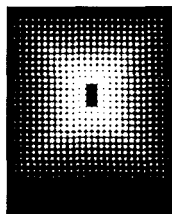
Advisory Board: W. Brauer D. Gries J. Stoer



H. Langmaack, W.-P. de Roever
J. Vytopil (Eds.)

Formal Techniques in Real-Time and Fault-Tolerant Systems

Third International Symposium
Organized Jointly with the Working Group
Provably Correct Systems – ProCoS
Lübeck, Germany, September 19-23, 1994
Proceedings



Springer-Verlag

Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos

Universität Karlsruhe

Postfach 69 80, Vincenz-Priessnitz-Straße 1, D-76131 Karlsruhe, Germany

Juris Hartmanis

Department of Computer Science, Cornell University

4130 Upson Hall, Ithaca, NY 14853, USA

Jan van Leeuwen

Department of Computer Science, Utrecht University

Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editors

Hans Langmaack

Willem-Paul de Roever

Institut für Informatik und Praktische Mathematik

Christian-Albrechts-Universität zu Kiel

Preußerstraße 1-9, D-24105 Kiel, Germany

Jan Vytöpil

BSO Advies, Churchill Laan 11, Postbus 2686

3500 GR Utrecht, The Netherlands; and

Vakgroep Informatica, Katholieke Universiteit Nijmegen

Toernooiveld 1, Postbus 9010, 6500 GL Nijmegen, The Netherlands

CR Subject Classification (1991): D.3.1, F.3.1, C.1.m, C.3, B.3.4, B.1.3, D.4.5, D.4.7

ISBN 3-540-58468-4 Springer-Verlag Berlin Heidelberg New York

CIP data applied for

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 1994

Printed in Germany

Typesetting: Camera-ready by author

SPIN: 10479099

45/3140-543210 - Printed on acid-free paper

Preface

The use of computers in safety-critical applications is increasing rapidly, as is interest in theoretical foundations for the design of reliable systems. Such systems are used in embedded applications and in interconnected networks. They are characterized both by their complexity and by the crucial need to manage this complexity using systematic principles of design.

Formal techniques constitute the foundation of a systematic design. They have beneficial applications throughout the engineering process, from the capture of requirements through specification, design, coding, and compilation, right down to the hardware that embeds the system into its environment.

This is the third in a series of international schools and symposia; the previous ones were at Warwick in 1989 and Nijmegen in 1992. The meetings during each school and symposium are devoted to considering the problems and the solutions in safe system design and to examining how well the use of formal techniques for design, analysis, and verification relates theory to practical realities.

Organization is done jointly with the CEC-supported Working Group Provably Correct Systems (ProCoS), which includes research institutions and industrial companies and is coordinated by C.A.R. Hoare, University of Oxford. Its overall objectives are to advance the state of the art of systematic design of complex heterogeneous systems, including both software and hardware, in particular, to reduce the risk of error in the specification, design, and implementation of embedded safety-critical systems. The previous ProCoS symposium took place at Avernæs, Fyn, in 1991.

Frau Marianne Tidick, Ministerin für Wissenschaft, Forschung und Kultur des Landes Schleswig-Holstein, has kindly overtaken patronage of the international school and symposium. We organizers are indebted to her for this great honour and support. We highly appreciate that Schleswig-Holstein's government acknowledges the importance of the themes discussed at this symposium for high technology research and industry.

The lectures and tutorials at the international school are directed at practicing systems designers, safety engineers, and those who set professional standards for their work. Our highly reputed school lecturers are C. Courcoubetis, FRT, Heraklion; F. Cristian, UCSD, San Diego; R. Kurshan, AT&T / Bell Labs, New Jersey; Nancy Leveson, Univ. of Washington, Seattle; J S. Moore, Computational Logic Inc., Austin; A. Pnueli, Weizmann Inst., Rehovot; C.A.R. Hoare, Univ. of Oxford; A.P. Ravn, DTH Lyngby; E.-R. Olderog, Univ. of Oldenburg; M. Fränzle, Univ. of Kiel; Jifeng He, Univ. of Oxford. We thank these invited lecturers for their willingness to serve.

We are very fortunate to have been able to invite symposium speakers of international renown: M.O. Rabin, Harvard Univ., Cambridge, Mass., and Hebrew Univ., Jerusalem; A. Pnueli, Weizmann Inst., Rehovot; J. Hooman, Eindhoven University of Technology; L. Lamport, DEC Lab., Palo Alto; F. Schneider, Cornell Univ., Ithaca, N.Y.; A. Mok, Univ. of Texas, Austin; J. Rushby, SRI International, Stanford; Ch. Zhou, IIST, Macau. Their splendid essays are collected in these proceedings.

We are especially grateful to G. Le Lann, INRIA, Le Chesnay, who took over the task of organizing the panel "Comparative Merits of Synchronous / Partially Synchronous / Asynchronous Models in the Case of Safety / Mission Critical Real Time Systems". We also thank the panelists A. Burns, Univ. of York, UK; F. Cristian, UCSD, San Diego; J. Rushby, SRI, Stanford; F. Schneider, Cornell Univ., Ithaca, N.Y.; J. Sifakis, IMAG-LGI, Grenoble; D. Shasha, New York University, N.Y., for their fruitful contributions.

The school and symposium would not have been complete without a proper tools demonstration. This was organized by Bettina Buth and concerned the following systems: STATEMATE, PVS and PC/DC, DST-Z Tools, VDM Domain Compiler, Production Cell, IFAD VDM-SL Toolbox, CSL, SVE, ITEX-DE, SDT, Tatzelwurm, and KIV.

Our calls for papers evoked 60 contributions. The programme committee selected 32 after a careful refereeing process. The reader may enjoy them in these proceedings. We thank all contributors, all members of the programme committee, and all external referees for their much appreciated voluntary help.

Apart from the selection procedure for papers, and writing this introduction, the present volume was put together by Anne Straßner, who also took care of the e-mail correspondence regarding submissions, the calls for papers, and general inquiries. In this task she was supported by Antonio Cau and Yassine Lakhneche.

Together with Hans Langmaack, Ruben-Benjamin Reincke set up the financial plan for this school and symposium, and submitted it to the Deutsche Forschungsgemeinschaft (DFG) and the Government of Schleswig-Holstein.

Claudia Herbers assisted Hans Langmaack in contacting the sponsors and took over much of the administrative work.

We also wish to thank Mirèse Willems cordially for her assistance.

Without the help of the aforementioned, and other persons, organizing this school and symposium would not have been possible. Many, many thanks to all of them!

Kiel, FRG	Hans Langmaack (chairman organization committee)
Nijmegen, NL	Willem-Paul de Roever (chairman programme committee)
July 1994	Jan Vytopil (publicity chair)

Organizing Committee:	M. Joseph (Univ. of Warwick)
	H. Langmaack (Univ. of Kiel, Chairman)
	A. Pnueli (Weizmann Inst., Rehovot)
	A. P. Ravn (DTH, Lyngby)
	W.-P. de Roever (Univ. of Kiel)
	J. Vytopil (Kath. Univ., Nijmegen)

Report of the PC Chair

Our calls for papers for this symposium on Formal Techniques in Real Time and Fault Tolerance resulted in 60 submissions. The programme committee selected 32 of them after a careful refereeing process. Since nowadays new selection procedures for conference submissions are being tried out, because the standard way by means of a meeting of the full programme committee has become too time consuming and too expensive, it may be worthwhile to describe (our experience with) the procedure followed at this symposium.

Papers were refereed using a large programme committee and many external referees to acquire as much expertise as possible. Papers were rated 0–5 (0: out of scope, 1: rejected, 2: discussable, 3: by all means discuss, 4: accepted, 5: accept by all means), with referees qualifying themselves by an A, B or C (A: a specialist sure of his opinion, B: not a specialist but still knowledgeable, C: not my field but I did my best).

In principle, a paper getting one or more “4” or “5” ratings, or getting at least three “3” ratings, was nominated for being accepted, unless it also received a “1” rating by a referee qualifying himself as an “A”, in which case it should be rejected if the latter rating stood up to scrutiny. So the main problem was, in fact, to check upon the correctness of 1/A ratings for papers which also received such high ratings, since if these reports were unjustified or contained errors in their argumentation, they should be discarded. For this one needs expertise. So we asked the PC members about their opinion in these matters, using e-mail. We also formed a small rump committee consisting of Amir Pnueli and the PC chair who met over four days to propose preliminary lists of accepted and rejected papers, and to check out such 1/A ratings. As it turned out, several such 1/A reports did show inconsistencies. Other cases we investigated concerned too low ratings for good papers; also internal inconsistencies and errors of judgement were found.

In fact, in some cases I also would have liked to discard some “4” ratings. However, this would have implied disregarding favourable opinions of some quite well known reviewers; we didn’t regard two specialists as enough of a critical mass for this task. A rump selection committee consisting of four or five experienced members would have had enough weight to credibly review referee reports and papers alike, in my opinion, replacing previous reports by new ones, but not one consisting of only two persons.

This leads to my conclusion that refereeing based on heavy usage of e-mail contacts alone is a dangerous course of action (there should be a group reviewing referee reports and papers alike) and should be complemented by a small rump committee of, say, four or five persons meeting for at least two full days (in our case, we needed at least three and a half days), due to the rather fluctuating quality of referee reports.

I thank Amir Pnueli for helping me out with the actual selection procedure, at short notice.

Programme Committee:

Ö. Babaoğlu (Univ. of Bologna)
 F. Cristian (UCSD, San Diego)
 M. Fränzle (Univ. of Kiel)
 C. A. R. Hoare (Univ. of Oxford)
 J. Hooman (Eindhoven Univ. of Technology)
 M. Joseph (Univ. of Warwick)
 B. Kurshan (AT&T/Bell Labs, New Jersey)
 I. Lee (Univ. of Pennsylvania)
 N. Lynch (MIT Cambridge, Mass.)
 A. Mok (Univ. of Texas, Austin)
 E. R. Olderog (Univ. of Oldenburg)
 A. Pnueli (Weizmann Inst., Rehovot)
 A. P. Ravn (DTH, Lyngby)
 W.-P. de Roever (Univ. of Kiel, Chairman)
 F. Schneider (Cornell Univ., Ithaca, N.Y.)
 J. Sifakis (IMAG-LGI, Grenoble)
 J. Vytopil (Kath. Univ., Nijmegen)

List of Referees:

E. Asarin	J. Daemen	Y. Lakhneche	W.-P. de Roever
Ö. Babaoğlu	E.A. Emerson	R. Langerak	M. Roncken
W. Baker	K. Engelhardt	K.G. Larsen	M. Schenke
A. Benveniste	M. Fränzle	I. Lee	H. Schepers
G. Berry	R. Gerth	Z. Liu	F.B. Schneider
B. Bloom	N. Halbwachs	N. Lynch	M. Siegel
F.S. de Boer	M. Hansen	O. Maler	J. Sifakis
A. Bouajjani	H. Hansson	F. Maraninchi	S.A. Smolka
J. Bowen	T.A. Henzinger	A. Mok	K. Spies
S. Brien	P.-H. Ho	B. Moszkowski	F.W. Vaandrager
E. Brinksma	J. Hooman	M. Müller-Olm	J.P.C. Verhoosel
M. Broy	C. Huizing	E.-R. Olderog	J. Vytopil
R. Budde	T. Janowski	J. Ostroff	M. Wahab
K.-H. Buth	B. Jonsson	O. Owe	M.J. Wiecezorek
P. Caspi	M. Joseph	C. Petersohn	P. Wolper
A. Cau	I. Kang	A. Pnueli	J. Yang
D. Clarke	J.-P. Katoen	S. Rajan	S. Yovine
J. Coenen	J. Kok	A.P. Ravn	S. Yuen
C. Courcoubetis	R.L.C. Koymans	P. Raymond	C. Zhou
F. Cristian	R. Kuiper	R.-B. Reincke	P. Zhou
M. Dal Cin	R. Kurshan	R. Robbana	J. Zwiers
W. Damm			

Patronage

Frau Marianne Tidick, die Ministerin für Wissenschaft, Forschung und Kultur
des Landes Schleswig-Holstein

Sponsors

The symposium would not have been accomplished without the very kind support and financial assistance of the following persons and organizations:

Commission of the European Communities

Deutsche Forschungsgemeinschaft (German Research Council)

Frau Marianne Tidick, die Ministerin für Wissenschaft, Forschung und Kultur
des Landes Schleswig-Holstein

Herr Peer Steinbrück, der Minister für Wirtschaft, Technik und Verkehr
des Landes Schleswig-Holstein

Christian-Albrechts-Universität zu Kiel

Stichting AFM, Nijmegen

as well as the associations and corporations listed below:

Linotype-Hell Aktiengesellschaft, Eschborn

Deutsche System-Technik GmbH, Kiel

Daimler-Benz AG, Stuttgart

Kölsch & Altmann Software Management Consulting GmbH, München

Kuhnke GmbH, Malente

Philips GmbH, Forschungslaboratorien, Aachen

Siemens AG, München

Schleswag AG, Rendsburg

Contents

Invited Lectures

Limor Fix and Fred B. Schneider <i>Hybrid Verification by Exploiting the Environment</i>	1
Jozef Hooman <i>Correctness of Real Time Systems by Construction</i>	19
Leslie Lamport and Stephan Merz <i>Specifying and Verifying Fault-Tolerant Systems</i>	41
Amir Pnueli <i>Development of Hybrid Systems</i>	77
Chaochen Zhou <i>Linear Duration Invariants</i>	86

Selected Presentations

Anish Arora <i>Efficient Reconfiguration of Trees: A Case Study in Methodical Design of Nonmasking Fault-Tolerant Programs</i>	110
Michael von der Beeck <i>A Comparison of Statecharts Variants</i>	128
Albert Benveniste, Bernard C. Levy, Eric Fabre, Paul Le Guernic <i>A Calculus of Stochastic Systems for the Specification, Simulation, and Hidden State Estimation of Hybrid Stochastic/Non-stochastic Systems</i>	149
Doeko Bosscher, Indra Polak, Frits Vaandrager <i>Verification of an Audio Control Protocol</i>	170
Ahmed Bouajjani, Rachid Echahed, Riadh Robbana <i>Verifying Invariance Properties of Timed Systems with Duration Variables</i>	193
Hanifa Boucheneb, Gérard Berthelot <i>Predicting Logical and Temporal Properties of Real-Time Systems Using Synchronized Elementary Nets</i>	211
Steven Bradley, William Henderson, David Kendall, Adrian Robson <i>Designing and Implementing Correct Real-Time Systems</i>	228
Manfred Broy and Ketil Stølen <i>Specification and Refinement of Finite Dataflow Networks – a Relational Approach</i>	247

Vered Gafni, Amiram Yehudai, Yishai A. Feldman <i>Activation-Oriented Specification of Real-Time Systems</i>	268
Jifeng He, C.A.R. Hoare, Martin Fränzle, Markus Müller-Olm, Ernst-Rüdiger Olderog, Michael Schenke, Michael R. Hansen, Anders P. Ravn, Hans Rischel <i>Provably Correct Systems</i>	288
Jifeng He, Jianping Zheng <i>Simulation Approach to Provably Correct Hardware Compilation</i>	336
Thomas A. Henzinger, Peter W. Kopke <i>Verification Methods for the Divergent Runs of Clock Systems</i>	351
Thomasz Janowski <i>Fault-Tolerant Bisimulation and Process Transformations</i>	373
Wil Janssen, Mannes Poel, Qiwen Xu, Job Zwiers <i>Layering of Real-Time Distributed Processes</i>	393
Bengt Jonsson, Chris Ho-Stuart, Yi Wang <i>Testing and Refinement for Nondeterministic and Probabilistic Processes</i>	418
Arjun Kapur, Thomas A. Henzinger, Zohar Manna, Amir Pnueli <i>Proving Safety Properties of Hybrid Systems</i>	431
Peter Kearney, Mark Utting <i>A Layered Real-Time Specification of a RISC Processor</i>	455
J.K. Kishore, R.S. Manjunatha, V.K. Agrawal, N.K. Malik, P.S. Goel <i>A Real Time Fault Tolerant Microprocessor based On-Board Computer System for INSAT-2 Spacecraft</i>	476
Yassine Lakhneche, Jozef Hooman <i>Reasoning about Durations in Metric Temporal Logic</i>	488
Gérard Le Lann <i>Scheduling in Critical Real-Time Systems: a Manifesto</i>	511
Zhiming Liu, Mathai Joseph <i>Stepwise Development of Fault-Tolerant Reactive Systems</i>	529
Oliver Maffeis, Paul Le Guernic <i>Distributed Implementation of SIGNAL: Scheduling & Graph Clustering</i>	547
Ryosei Mori, Naoki Yonezaki <i>Derivation of the Input Conditional Formula from a Reactive System Specification in Temporal Logic</i>	567

Simin Nadjm-Tehrani, Jan-Erik Strömberg <i>From Physical Modelling to Compositional Models of Hybrid Systems</i>	583
Michael Schenke <i>Specification and Transformation of Reactive Systems with Time Restrictions and Concurrency</i>	605
R.K. Shyamasundar, S. Ramesh <i>Languages for Reactive Specifications: Synchrony Vs Asynchrony</i>	621
Henny B. Sipma, Zohar Manna <i>Specification and Verification of Controlled Systems</i>	641
Jens Ulrik Skakkebæk, Natarajan Shankar <i>Towards a Duration Calculus Proof Assistant in PVS</i>	660
Yi Wang <i>Algebraic Reasoning for Real-Time Probabilistic Processes with Uncertain Information</i>	680
Thomas Wilke <i>Specifying Timed State Sequences in Powerful Decidable Logics and Timed Automata</i>	694
Huiqun Yu, Paritosh K. Pandya, Yongqiang Sun <i>A Calculus for Hybrid Sampled Data Systems</i>	716
Xinyao Yu, Ji Wang, Chaochen Zhou, Paritosh K. Pandya <i>Formal Design of Hybrid Systems</i>	738
Yuhua Zheng, Chaochen Zhou <i>A Formal Proof of the Deadline Driven Scheduler</i>	756
Tools Demonstration	
Berner & Mattner Software Produkte GmbH, Ottobrunn (Susanne Wiefel, Gerhard Trefz) <i>STATEMATE</i>	776
Computer Science Laboratory SRI International, Menlo Park (John Rushby), Technical University of Denmark, Lyngby (Jens Ulrik Skakkebæk) <i>The PVS Verification System and PC/DC</i>	777
Deutsche System-Technik, Kiel (Hans-Martin Hörcher) <i>The DST Z-Tools</i>	778
Deutsche System-Technik, Kiel (Hans-Martin Hörcher), Fachhochschule Wedel (Uwe Schmidt) <i>The VDM Domain Compiler</i>	779

Forschungszentrum Karlsruhe (Thomas Lindner) <i>Case Study Production Cell</i>	780
Institute of Applied Computer Science, Odense (Poul Boegh Lassen) <i>IFAD VDM-SL Toolbox</i>	781
Siemens AG, München (K. Winkelmann, K. Noekel) <i>Control Specification Language - CSL</i>	782
Siemens AG, München (K. Winkelmann, Th. Filkorn) <i>System Verification Environment - SVE</i>	783
Telelogic Malmø AB, Malmø <i>ITEX-DE: A TTCN Development Environment</i>	784
Telelogic Malmø AB, Malmø <i>SDT: The SDL Design Tool</i>	785
Universität Karlsruhe (Thomas Käußl, Stefan Klingenberg) <i>Tatzelwurm</i>	786
Universität Karlsruhe (Wolfgang Reif, Gerhard Schellhorn, Kurt Stenzel) <i>Formal Specification and Verification Using KIV</i>	787