

ICFEM'97

Proceedings

First IEEE International Conference Conference on
Formal Engineering Methods

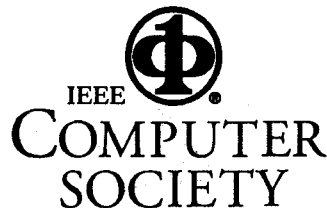
Hiroshima, Japan
November 12 – 14, 1997

Sponsored by

IEEE Computer Society
IEEE Computer Society Technical Committee on Complexity in Computing

In cooperation with

Software Engineers Association of Japan
Information Processing Society of Japan
Hiroshima City University
Electric Technology Research Foundation of Chugoku
Mazda Foundation
IEEE Asia-Pacific Region



Los Alamitos, California

Washington • Brussels • Tokyo

Copyright © 1997 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number PR08002
ISBN 0-8186-8002-4
ISBN 0-8186-8003-4 (case)
ISBN 0-8186-8004-0 (microfiche)
IEEE Order Plan Catalog Number 97TB100188
Library of Congress Number 97-74199

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1-714-821-8380
Fax: + 1-714-821-4641
E-mail: cs.books@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1-908-981-1393
Fax: + 1-908-981-9667
mis.custserv@computer.org

IEEE Computer Society
13, Avenue de l'Aquilon
B-1200 Brussels
BELGIUM
Tel: + 32-2-770-2198
Fax: + 32-2-770-8505
euro.ofc@computer.org

IEEE Computer Society
Ooshima Building
2-19-1 Minami-Aoyama
Minato-ku, Tokyo 107
JAPAN
Tel: + 81-3-3408-3118
Fax: + 81-3-3408-3553
tokyo.ofc@computer.org

Editorial production by Bob Werner

Cover art design and production by Alex Torres

Printed in the United States of America by The Printing House

IEEE 
COMPUTER
SOCIETY



Table of Contents

First IEEE International Conference on Formal Engineering Methods — ICFEM'97

Message from the General Chair	ix
Conference Committee	x
Program Committee	xi
Tutorials	
Formal Methods for Developing Reliable Software in Industry	2
<i>Speaker: S. Otsuki</i>	
/	
Hazard Analysis: Determining Context for the Use of Formal Methods	3
<i>Speaker: P. Lindsay</i>	
Invited Speaker	
Whither Formal Methods: A Plea to Investigate New Applications	5
<i>C. Jones</i>	
Parallel Session A: Object-Orientation	
Towards a Rigorous Object-Oriented Analysis and Design Method	7
<i>R. France, J. Bruel, M. Larrondo-Petrie, E. Grant, M. Saksena</i>	
Hybrid Object-Oriented Real-Time Software Development with VDM ⁺⁺	17
<i>J. van Katwijk, E. Dürr, S. Goldsack</i>	
Session B: Method Integration 1	
Towards a Formal Semantics for an Integrated SA/RT & Z Specification Language	28
<i>D. Scholz, C. Petersohn</i>	
A Pragmatic, Rigorous Integration of Structural and Behavioral Modeling Notations	38
<i>D. Berry, M. Weber</i>	
Parallel Session A: Protocols	
Formal Automatic Verification of Authentication Cryptographic Protocols	50
<i>M. Debbabi, M. Mejri, N. Tawbi, I. Yahmadi</i>	
Incremental Specification of Telecommunication Services	60
<i>B. Mermet, D. Méry</i>	
Generic Engineering of Communication Protocols — Current Experience and Future Issues	70
<i>B. Geppert, F. Rößler</i>	

Parallel Session B: Testing

Test Case Design Based on Z and the Classification-Tree Method.....	81
<i>H. Singh, M. Conrad, S. Sadeghipour</i>	
A Formal Approach to Testing LUSTRE Specifications	91
<i>I. Parissis</i>	
CASTING: A Formally Based Software Test Generation Method.....	101
<i>L. Van Aertryck, M. Benveniste, D. Le Métayer</i>	

Invited Speaker

Formally Specifying and Verifying Real-Time Systems.....	112
<i>R. Kemmerer</i>	

Parallel Session A: Verification

Using CARE to Construct Verified Software.....	122
<i>P. Lindsay, D. Hemer</i>	
A Simple Program whose Derivation and Proof is Also.....	132
<i>J. Xue, R. Davis</i>	
Systematic Formal Verification of Interpreters.....	140
<i>D. Cyrluk, J. Rushby, M. Srivas</i>	

Parallel Session B: Experience 1

The Specification-Based Testing of a Trusted Kernel: MK++.....	151
<i>R. Ford, W. Bevier, R. Simon, L. Smith</i>	
Formalizing Process Scheduling Requirements for an Aircraft Operational Flight Program	161
<i>J. Dong, N. Fulton, L. Zucconi, J. Colton</i>	

Invited Speaker

An Overview of CAFE Specification Environment — An Algebraic Approach for Creating, Verifying, and Maintaining Formal Specifications over Networks	170
<i>K. Futatsugi, A. Nakagawa</i>	

Parallel Session A: Embedded Systems

A Methodological Approach to the Requirement Specification of Embedded Systems	183
<i>F. Lattemann, E. Lehmann</i>	
Specification and Analysis of System Level Inter-Component Communication	192
<i>M. Heimdahl, J. Thompson</i>	

Parallel Session B: Method Integration 2

Refinement of Information Flow Architectures	203
<i>J. Philipps, B. Rumpe</i>	

Frameworks in <i>Catalysis</i> : Pictorial Notation and Formal Semantics.....	213
<i>K. Lau, M. Ornaghi, A. Wills</i>	

Parallel Session A: Applications

Development and Application of a Formal Agent Framework	222
<i>M. d'Inverno, M. Luck</i>	

Formal Specification and Verification of the MISSI Sender and Local Cache using SPIN	232
<i>M. Barjaktarovic</i>	

Parallel Session B: Requirements to Specifications

Automatic Generation of Formal Specification from Requirements Definition	243
<i>L. Jin, H. Zhu</i>	

A Generic Approach to the Formal Specification of Requirements.....	252
<i>C. Peper, R. Gotzhein, M. Kronenburg</i>	

Invited Speaker

Michael Jackson's Problem Frames: Towards Methodological Principles of Selecting and Applying Formal Software Development Techniques and Tools	263
<i>D. Bjørner, S. Koussoube, R. Noussi, G. Satchok</i>	

Parallel Session A: Combining State and Process Algebras

An Operational Semantics for ZCCS.....	272
<i>A. Galloway, W. Stoddart</i>	

The State-Based CCS Semantics for Concurrent Z Specification.....	283
<i>K. Taguchi, K. Araki</i>	

Refinement and Verification of Concurrent Systems Specified in Object-Z and CSP.....	293
<i>G. Smith, J. Derrick</i>	

Parallel Session B: Experience 2

Formal Specification of Dynamic Constraints with the B Method	304
<i>H. Habrias, B. Griech</i>	

Software Measurement and Formal Methods: A Case Study Centered on TRIO+ Specifications	315
<i>L. Briand, S. Morasca</i>	

Panel Session

The Future of Formal Methods: Verification? Error Detection? Or What? <i>Chair: J. Staples</i> <i>Participants: J. Rushby, C. Heitmeyer, K. Araki</i>	
---	--

Index of Authors	327
-------------------------------	-----