

---

# **FORMAL TECHNIQUES FOR NETWORKED AND DISTRIBUTED SYSTEMS**

## **IFIP - The International Federation for Information Processing**

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- open conferences;
- working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

# FORMAL TECHNIQUES FOR NETWORKED AND DISTRIBUTED SYSTEMS

**FORTE 2001**

*IFIP TC6/WG6.1 — 21<sup>st</sup> International Conference on  
Formal Techniques for Networked and Distributed Systems  
August 28-31, 2001, Cheju Island, Korea*

*Edited by*

**Myungchul Kim**

*Information and Communications University (ICU)  
Korea*

**Byoungmoon Chin**

*Telecommunications Technology Association (TTA)  
Korea*

**Sungwon Kang**

*Korea Telecom (KT)  
Korea*

**Danhyung Lee**

*Korea IT Industry Promotion Agency (KIPA)  
Korea*

---

KLUWER ACADEMIC PUBLISHERS

NEW YORK, BOSTON, DORDRECHT, LONDON, MOSCOW

eBook ISBN: 0-3064-7003-9  
Print ISBN 0-7923-7470-3

©2002 by **IFIP International Federation for Information Processing**

All rights reserved

No part of this eBook may be reproduced or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without written consent from the Publisher

Created in the United States of America

Visit Kluwer Online at: <http://www.kluweronline.com>  
and Kluwer's eBookstore at: <http://www.ebooks.kluweronline.com>

*The original version of the book frontmatter was revised:  
The copyright line was incorrect. The Erratum  
to the book frontmatter is available at  
DOI: [10.1007/978-0-306-47003-5\\_29](https://doi.org/10.1007/978-0-306-47003-5_29)*

# Contents

Preface	xi
Program Committee and Reviewers	xiii

## Part One

### FORMAL METHODS IN SOFTWARE DEVELOPMENT I

1. Automated Derivation of ILP Implementations from SDL Specifications <i>S. Twarok, P. Langendoerfer and H. Koenig</i>	3
2. Stepwise Design with Message Sequence Charts <i>F. Khendek, S. Bourduas and D. Vincent</i>	19
3. Formal Synthesis and Control of Soft Embedded Real-Time Systems <i>P.-A. Hsiung</i>	35

## Part Two

### DISTRIBUTED SYSTEMS TESTING

4. Towards a Formal Framework for Interoperability Testing <i>C. Viho, S. Barbin and L. Tanguy</i>	53
5. Distributed Test using Logical Clock <i>Y. J. Choi, H. Y. Youn, S. Seol and S. J. Yoo</i>	69
6. Diagnosing Multiple Faults in Communicating Finite State Machines <i>K. El-Fakih, N. Yevtushenko and G. v. Bochmann</i>	85
7. From Active to Passive : Progress in Testing of Internet Routing Protocols <i>J. Wu, Y. Zhao and X. Yin</i>	101

## Part Three

### TIMED AUTOMATA

8. Time and Action Lock Freedom Properties for Timed Automata <i>H. Bowman</i>	119
---	-----

9. Compiling Real-Time Scenarios into a Timed Automaton	135
<i>A. Salah, R. Dssouli and G. Lapalme</i>	

10. Deriving Parameter Conditions for Periodic Timed Automata Satisfying Real-Time Temporal Logic Formulas	151
<i>A. Nakata and T. Higashino</i>	

## **Part Four**

### **PROCESS ALGEBRA**

11. PAMR: A Process Algebra for the Management of Resources in Concurrent Systems	169
<i>M. Núñez and I. Rodriguez</i>	

12. A Symbolic Semantics and Bisimulation for Full LOTOS	185
<i>M. Calder and C. Shankland</i>	

13. Implementing a Modal Logic over Data and Processes using XTL	201
<i>J. Bryans and C. Shankland</i>	

## **Part Five**

### **APPLICATIONS OF VERIFICATION**

14. Formal Verification of Peephole Optimizations in Asynchronous Circuits	219
<i>X. Kong and R. Negulescu</i>	

15. Symbolic Verification of Complex Real-Time Systems with Clock-Restriction Diagram	235
<i>F. Wang</i>	

16. Verifying a Sliding Window Protocol using PVS	251
<i>V. Rusu</i>	

## **Part Six**

### **TEST SEQUENCE DERIVATION**

17. Test Sequence Selection	269
<i>D. Lee and R. Hao</i>	

18. Executable Test Sequence for the Protocol Data Flow Property	285
<i>W.-H. Chen</i>	

19. A Method to Generate Conformance Test Sequences for FSM with Timer System Call <i>T. Mori, K. Tokuda, H. Tada, M. Higuchi and T Higashino</i>	301
---	-----

## **Part Seven**

### **FORMAL METHODS IN SOFTWARE DEVELOPMENT II**

20. A Tool for Generating Specifications from a Family of Formal Requirements <i>J. Brederke</i>	319
21. Patterns and Rules for Behavioural Subtyping <i>H. Wehrheim</i>	335

## **Part Eight**

### **THEORIES OF VERIFICATION**

22. Verification of Dense Time Properties using Theories of Untimed Process Algebra <i>M. Luukkainen</i>	353
23. Testing Liveness Properties: Approximating Liveness Properties by Safety Properties <i>U. Ultes-Nitsche and S. St James</i>	369
24. SVL: A Scripting Language for Compositional Verification <i>H. Garavel and F. Lang</i>	377

## **Part Nine**

### **INVITED PAPERS**

25. On Formal Techniques in Protocol Engineering – Example Challenges <i>D. Bjørner</i>	395
26. A PKI-Based End-to-End Secure Infrastructure for Mobile E-Commerce <i>T.-W. Cheung and S. T. Chanson</i>	421
27. A Family of Resource-Bound Real-Time Process Algebras <i>I. Lee, J.-Y. Choi, H. H. Kwak, A. Philippou and O. Sokolsky</i>	443
28. Survivability Analysis of Networked Systems <i>J. M. Wing</i>	459
Erratum to: Formal Techniques for Networked and Distributed Systems <i>M. Kim, B. Chin, S. Kang and D. Lee</i>	E1



## Preface

FORTE 2001, formerly FORTE/PSTV conference, is a combined conference of FORTE (Formal Description Techniques for Distributed Systems and Communication Protocols) and PSTV (Protocol Specification, Testing and Verification) conferences. This year the conference has a new name FORTE (Formal Techniques for Networked and Distributed Systems). The previous FORTE began in 1989 and the PSTV conference in 1981. Therefore the new FORTE conference actually has a long history of 21 years.

The purpose of this conference is to introduce theories and formal techniques applicable to various engineering stages of networked and distributed systems and to share applications and experiences of them. This FORTE 2001 conference proceedings contains 24 refereed papers and 4 invited papers on the subjects. We regret that many good papers submitted could not be published in this volume due to the lack of space.

FORTE 2001 was organized under the auspices of IFIP WG 6.1 by Information and Communications University of Korea. It was financially supported by Ministry of Information and Communication of Korea.

We would like to thank every author who submitted a paper to FORTE 2001 and thank the reviewers who generously spent their time on reviewing. Special thanks are due to the reviewers who kindly conducted additional reviews for rigorous review process within a very short time frame. We would like to thank Prof. Guy Leduc, the chairman of IFIP WG 6.1, who made valuable suggestions and shared his experiences for conference organization.

This year we have seen exceptionally concerted efforts of the program committee to make FORTE 2001 a successful conference. We thank each one of the program committee for their contribution and cooperation. The enthusiasm and dedication the program committee showed has made us believe that FORTE will remain a prestigious conference with quality and distinction for a long time in the future.

*Myungchul Kim*  
*Byoungmoon Chin*  
*Sungwon Kang*  
*Danhyung Lee*

*Cheju Island, Korea*

# **Program Committee and Reviewers**

## **Program Committee Co-Chairmen**

Myungchul Kim (ICU, Korea)  
Byoungmoon Chin (TTA, Korea)  
Sungwon Kang (KT, Korea)  
Danhyung Lee (KIPA, Korea)

## **Program Committee**

G. v. Bochmann (Univ. of Ottawa, Canada)  
T. Bolognesi (IEI, Italy)  
H. Bowman (Univ. of Kent, UK)  
E. Brinksma (Univ. of Twente, Netherlands)  
S. Budkowski (INT, France)  
A. Cavalli (INT, France)  
S. D. Cha (KAIST, Korea)  
S. Chanson (Hong Kong Univ. of Science and Technology, China)  
E. H. Choi (Korea Telecom, Korea)  
J. Y. Choi (Korea Univ., Korea)  
J. P. Courtiat (LAAS-CNRS, France)  
R. Dssouli (Univ. of Montreal, Canada)  
D. Frutos-Escrig (Universidad Complutense - Madrid, Spain)  
S. Fischer (International Univ., Germany)  
R. Groz (France Telecom R&D, France)  
R. Gotzhein (Univ. of Kaiserslautern, Germany)  
T. Higashino (Osaka Univ., Japan)  
D. Hogrefe (Univ. of Luebeck, Germany)  
G. J. Holzmann (Bell Labs, USA)  
J. K. Kim (ETRI, Korea)  
S. U. Kim (Pukyung Univ., Korea)  
H. Koenig (BTU, Germany)  
R. Lai (La Trobe Univ., Australia)  
D. Latella (C.N.R., 1st. CNUCE, Italy)  
G. Leduc (Univ. of Liege, Belgium)  
D. Lee (Bell Labs, USA)  
D. I. Lee (KJIST, Korea)  
J. Y. Lee (Yonsei Univ., Korea)  
L. Logrippo (Univ. of Ottawa, Canada)  
E. Najm (ENST, France)

D. Peled (Bell Labs, USA)  
 A. Petrenko (CRIM, Canada)  
 O. Rafiq (Univ. of Pau, France)  
 K. Suzuki (Advanced Comm. Co., Japan)  
 K. Tarnay (Nokia, Hungary)  
 R. Tenney (Univ. of Massachusetts, USA)  
 K. Turner (Univ. of Stirling, UK)  
 U. Ultes-Nitsche (Univ. of Southampton, UK)  
 S. Vuong (Univ. of British Columbia, Canada)  
 J. Wu (Tsinghua Univ., China)  
 N. Yevtushenko (Tomsk Univ., Russia)

### Further Reviewers

D. Amyot	P. Gradit	J.- F. Monin
R. Andrade	S. Gruner	M. Nakamura
A. Bailly	R. Hao	A. Nakata
A. Bertolino	M. Heiner	H. Neukirchen
S. Boroday	H. Hermanns	S. Prokopenko
L. Cacciari	M. Higuchi	R. Pugliese
O. Catrina	I. Hwang	Y.- M. Quemener
D. Chen	A. Idoue	C. Rinderknecht
R. G. Clark	P. Janowski	A. Salah
M. Ebner	T. Kato	J. Sincennes
A. En-Nouaary	R. Langerak	A. Verdejo
A. Fantechi	C. Liu	F. Vernadat
A. Fontaine	L. Llana	H. Yamaguchi
N. De Francesco	S. Maag	G. Yang
C. Gervy	E. Magill	H. Yokota
S. Gnesi	J.' C. Maldonado	J. Zhu
J. Grabowski	M. Massink	