FORMAL METHODS FOR DISTRIBUTED SYSTEM DEVELOPMENT

FORTE / PSTV 2000
IFIP TC6 WG6.1 Joint International Conference on Formal Description Techniques for Distributed Systems and Communication Protocols (FORTE XIII) and Protocol Specification, Testing and Verification (PSTV XX) October 10–13, 2000, Pisa, Italy

Edited by

Tommaso Bolognesi
Consiglio Nazionale delle Ricerche (CNR)
Istituto di Elaborazione dell'Informazione (IEI)
Italy

Diego Latella
Consiglio Nazionale delle Ricerche (CNR)
Istituto CNUCE
Italy

KLUWER ACADEMIC PUBLISHERS
BOSTON / DORDRECHT / LONDON

Distributors for North, Central and South America:
Kluwer Academic Publishers
101 Philip Drive
Assinippi Park
Norwell, Massachusetts 02061 USA
Telephone (781) 871-6600
Fax (781) 871-6528
E-Mail <kluwer@wkap.com>

Distributors for all other countries:
Kluwer Academic Publishers Group
Distribution Centre
Post Office Box 322
3300 AH Dordrecht, THE NETHERLANDS
Telephone 31 78 6392 392
Fax 31 78 6546 474
E-Mail <services@wkap.nl>


Electronic Services <http://www.wkap.nl>

Library of Congress Cataloging-in-Publication Data

IFIP TC6 WG6.1 Joint International Conference on Formal Description Techniques for Distributed Systems and Communication Protocols and Protocol Specification, Testing and Verification (2000 : Pisa, Italy)

Formal methods for distributed system development : October 10-13, 2000, Pisa, Italy / FORTE/PSTV 2000, IFIP TC6 WG6.1 Joint International Conference on Formal Description Techniques for Distributed Systems and Communication Protocols and Protocol Specification, Testing and Verification ; edited by Tommaso Bolognesi, Diego Latella.

p. cm. — (IFIP ; 55)
Includes bibliographical references.
ISBN 0-7923-7968-3 (alk. paper)
1. Electronic data processing—Distributed processing—Congresses. 2. Formal methods (Computer science)—Congresses. I. Bolognesi, Tommaso. II. Latella, Diego. III. Title. IV. International Federation for Information Processing (Series) ; 55.

QA76.9.D5 I33845 2000
004'.36—dc21 00-061057

Printed on acid-free paper.

Printed in the United States of America.

Contents

Preface

The 20th anniversary of the IFIP WG6.1 Joint International Conference on Formal Methods for Distributed Systems and Communication Protocols (FORTE XIII / PSTV XX) was celebrated by the year 2000 edition of the Conference, which was held for the first time in Italy, at Pisa, October 10-13, 2000. In devising the subtitle for this special edition -- 'Formal Methods – Implementation Under Test' -- we wanted to convey two main concepts that, in our opinion, are reflected in the contents of this book. First, the early, pioneering phases in the development of Formal Methods (FM's), with their conflicts between evangelistic and agnostic attitudes, with their over-optimistic applications to toy examples and over-skeptical views about scalability to industrial cases, with their misconceptions and myths..., all this is essentially over. Many FM's have successfully reached their maturity, having been 'implemented' into concrete development practice: a number of papers in this book report about successful experiences in specifying and verifying real distributed systems and protocols. Second, one of the several myths about FM's – the fact that their adoption would eventually eliminate the need for testing – is still quite far from becoming a reality, and, again, this book indicates that testing theory and applications are still remarkably healthy.

A total of 63 papers have been submitted to FORTE/PSTV 2000, out of which the Programme Committee has selected 22 for presentation at the Conference and inclusion in the Proceedings. The central themes of this book are the theory and practice of distributed system Verification (with Model Checking playing a predominant role), and Testing. Several papers deal with the analysis of communication protocols, and some of them address, in particular, multicast protocols. Other papers deal with the

specification, implementation and testing of hardware systems. The issue of formal semantics is also covered, but to a lesser extent than in past editions of the Conference, as a further indication of the shift of emphasis from the definition to the application of FM's. Three internationally recognized speakers, namely Rocco De Nicola, Fausto Giunchiglia, and John Rushby, have provided invited contributions on Verification and on Security protocols: these are collected in the last part of the book.

The Conference has been complemented by two tutorial/advanced seminar tracks including a total of six presentations:

- E. Allen Emerson: Model Checking.
- Jan Tretmans: Specification based testing with formal methods -- from theory via tools to applications.
- Marta Kwiatkowska: Modelling and verification of probabilistic real time systems using probabilistic timed automata.
- Hartmut Koenig, Peter Langendoerfer: Automated Derivation of Efficient Implementations from Formal Protocol Specifications.
- R. Gotzhein, E. Börger, A. Prinz: Abstract State Machines and their Applications.
- C. Petitpierre: Bridging the Gap Between Formal Methods and the Implementation Process.

Finally, a multidisciplinary Satellite Workshop -- 'Formal Methods Elsewhere' – was held on October 10, devoted to applications of FM's to areas other than communication protocols and distributed systems, such as physics, chemistry, biology, social sciences, arts and humanities, music. After two decades, FM's are perhaps ready to spread out of their native territory and, at the turn of the millenium, invade new exciting areas of research, for a wider exploitation of the huge intellectual investment behind their definition.

Tommaso Bolognesi
Diego Latella