Lecture Notes in Computer Science 4355

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Jacques Julliand Olga Kouchnarenko (Eds.)

B 2007: Formal Specification and Development in B

7th International Conference of B Users
Besançon, France, January 17-19, 2007
Proceedings

Springer

Volume Editors

Jacques Julliand
Laboratoire d'Informatique de l'Université de Franche-Comté
CNRS, FRE 2661
16 route de Gray
25030 Besançon Cedex, France
E-mail: jacques.julliand@lifc.univ-fcomte.fr

Olga Kouchnarenko
Laboratoire d'Informatique de l'Université de Franche-Comté
CNRS, FRE 2661
16 route de Gray
25030 Besançon Cedex, France
E-mail: olga.kouchnarenko@lifc.univ-fcomte.fr

Library of Congress Control Number: 2006938539

CR Subject Classification (1998): D.2.1, D.2.2, D.2.4, F.3.1, F.4.2-3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-68760-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-68760-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11955757 06/3142 5 4 3 2 1 0

Preface

These proceedings record the papers presented at the Seventh International Conference of B Users (B 2007), held in the city of Besançon in the east of France. This conference was built on the success of the previous six conferences in this series, B 1996, held at the University of Nantes, France; B 1998, held at the University of Montpellier, France; ZB 2000, held at the University of York, UK; ZB 2002, held at the University of Grenoble, France; ZB 2003, held at the University of Turku, Finland; ZB 2005 held at the University of Surrey, Guildford, UK. B 2007 was held in January at the University of Franche-Comté, Besançon, France, hosted by the Computer Science Department (LIFC). LIFC has always placed particular emphasis on the applicability of its research and its relationship with industrial partners. In this context, it created in 2003 a company called LEIRIOS Technologies, which produces an automatic test generator tool (LTG) from models described in the B specification language. Other members of LIFC work on extensions of the B method for specifying and verifying dynamic properties.

All the submitted papers in these proceedings were peer reviewed by at least three reviewers drawn from the B committee, depending on the subject matter of the paper. The authors of the papers for B 2007 were from Australia, Canada, Finland, Germany, France, Switzerland, and the UK. The conference featured a range of contributions by distinguished invited speakers drawn from both industry and academia. The invited speakers addressed significant recent industrial applications of formal methods, as well as important academic advances serving to enhance their potency and widen their applicability.

The topics of interest to the conference included: industrial applications and case studies using B; integration of model-based specification methods in the software development lifecycle; derivation of hardware–software architecture from model-based specifications; expressing and validating requirements through formal models, in particular verifying security policies; theoretical issues in formal development (e.g., issues in refinement, proof process, or proof validation); model-based software testing versus proof-oriented development; tools supporting the B method; development by composition of specifications; validation of assembly of COTS by model-based specification methods; B extensions and/or standardization.

Our invited speakers for B 2007 were drawn from France, Ireland, Switzerland and the United States of America. Leslie Lamport is an American computer scientist. The papers by L. Lamport produced original and insightful concepts and algorithms to solve many fundamental problems in distributed systems. L. Lamport applies an elegant mathematical approach to very practical engineering problems. Joseph Morris, from Dublin City University, Ireland, is especially interested in developing mathematical methods of extracting guaranteed correct programs from formal specifications. David Chemouil works in the Flight

Software Department at the French Space Agency (CNES) in Toulouse. His activities include monitoring the development of flight software contracted by CNES and carrying out R&D on flight-software engineering. Paul Gibson from the Department of Computer Science at the National University of Ireland, Maynooth, is an expert in feature interaction. He is a consultant for the Irish government for the Irish e-voting system. He knows this system and its bugs very well and has presented the requirements for its formal – safe and secure – development. Laurent Voisin from the Swiss Federal Institute of Technology, Zurich, a member of the European IST project RODIN (Rigorous Open Development Environment for Complex Systems), presented Event-B modelling with the Rodin platform.

Besides its formal sessions, the conference included tool sessions, demonstrations, exhibitions, an industrial event and tutorials. In particular, the industrial event was constituted of an industrial invited talk and five communications of industry members. Eddie Jaffuel, senior consultant in LEIRIOS Technologies, talked about the specification process for model-based testing generation. Ian Oliver at Nokia Research Center in Finland presented experiences in using B and UML together in industrial developments. Mathieu Clabaut of Systerel Company presented a tool for firewall administration. Daniel Dollé and Didier Essaimé of Siemens Transportation Systems in Montrouge, France, used B in large-scale projects such as the Canarsie Line CBTC. Sarah Hoffman, Sophie Gabriele, Germain Haugou of STMicroelectronics and Lilian Burdy of ClearSy presented the use of the B method for the construction of microkernel-based systems. Neil Evans and Wilson Ifill of AWE (Atomic Weapons Establishment) in the UK presented a synthesis and some perspectives about the use of B at AWE for hardware verifications.

The B 2007 conference was initiated by the International B Conference Steering Committee (APCB). The University of Franche-Comté and the Computer Science Department LIFC provided local organization. Without the great support from local staff at the University of Franche-Comté, B 2007 would not have been possible. In particular, much of the local organization was undertaken by Bruno Tatibouët with the assistance of Brigitte Bataillard, Christine Bigey, Alain Giorgetti, Ahmed Hammad, Pierre-Alain Masson, Hassan Mountassir, François Piat and Laurent Steck. B 2007 was sponsored by Alstom, ClearSy System Engineering, INRETS (French National Institute for Transport and Safety Research), INRIA (National Institute of Research in Automatic and Computer Science), LEIRIOS Technologies, PARKEON (Parking Space Management Solution Industry), RATP, the local council of Doubs, the regional council of Franche-Comté and the town council of Besançon. We are grateful to all those who contributed to the success of the conference.

Online information concerning the conference is available under the following URL: `http://lifc.univ-fcomte.fr/b2007`

This web site and `http://www-lsr.imag.fr/B/` provide links to further online resources concerning the B method.

We hope that all participants and other interested readers benefit scientifically from these proceedings and also find them stimulating in the process.

October 2006

Jacques Julliand
Olga Kouchnarenko
Fabrice Bouquet
Marie-Laure Potet

Organization

Executive Committee

B 2007 was organized by the department of Computer Science, University of Franche-Comté.

Conference and Program Chair: Jacques Julliand
Co-chair and Invited Talks: Olga Kouchnarenko
Industrial Event: Marie-Laure Potet (University of Grenoble, France)
Tools Session: Fabrice Bouquet
Organizing Chair: Bruno Tatibouët
Proceedings: Alain Giorgetti
Web Site: François Piat
Demonstrations: Laurent Steck

Program Committee

Program Chair: Jacques Julliand, LIFC, University of Franche-Comté, France
Co-chair: Olga Kouchnarenko, LIFC, University of Franche-Comté, France

Richard Banach, University of Manchester, UK
Didier Bert, CNRS, University of Grenoble, France
Juan Bicarregui, CLRC, Oxfordshire, UK
Lilian Burdy, ClearSy, France
Michael Butler, University of Southampton, UK
Dominique Cansell, LORIA, University of Metz, France
Daniel Dollé, Siemens Transportation Systems, Paris, France
Steve Dunne, University of Teesside, UK
Mamoun Filali, CNRS, IRIT, Toulouse, France
Marc Frappier, University of Sherbrooke, Canada
Andy Galloway, University of York, UK
Henri Habrias, LINA, Université de Nantes, France
Regine Laleau, LACL, IUT Fontainebleau, France
Jean-Louis Lanet, Gemplus, France
Annabelle McIver, Macquarie University, Sydney, Australia
Luis-Fernando Mejia, Alstom Transport Signalisation, Paris, France
Marie-Laure Potet, University of Grenoble (Chair of industrial half-day)
Ken Robinson, University of New South Wales, Australia
Emil Sekerinski, McMaster University, Ontario, Canada
Helen Treharne, University of Surrey, UK
Mark Utting, University of Waikato, New Zealand
Véronique Viguié Donzeau-Gouge, CNAM, Paris, France
Marina Waldén, Åbo Akademi University, Turku, Finland

External Referees

Pascal André, University of Nantes, France
Christian Attiogbé, University of Nantes, France
Julien Brunel, Université Paul Sabatier, Toulouse, France
Xavier Crégut, ENSEEIHT, Toulouse, France
Andy Edmunds, University of Southampton, UK
Alain Giorgetti, University of Franche-Comté, Besançon, France
Pierre-Alain Masson, University of Franche-Comté, France
Hassan Mountassir, University of Franche-Comté, France
Mike Poppleton, University of Southampton, UK
Antoine Requet, Gemalto, Marseille, France
Jean-François Rolland, Université Paul Sabatier, Toulouse, France
Colin Snook, University of Southampton, UK
Bill Stoddart, University of Teesside, UK
David Streader, University of Waikato, New Zealand
Bruno Tatibouët, University of Franche-Comté, Besançon, France
Guy Vidal-Naquet, Ecole Supérieure d'Electricité, Gif-sur-Yvette, France

Support

B 2007 greatly benefited from the support of the following organizations:

CNRS
INRIA
LIFC
Ministère de l'Éducation Nationale
University of Franche-Comté

and sponsorship from:

Alstom
ClearSy System Engineering
INRETS
LEIRIOS Technologies
PARKEON
RATP
Local Council of Doubs
Regional Council of Franche-Comté
Town Council of Besançon

Table of Contents

Invited Talks

Regular Papers

Industrial Papers

Tool Papers

Invited Talk