Lecture Notes in Computer Science 2272

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

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Didier Bert Jonathan P. Bowen
Martin C. Henson Ken Robinson (Eds.)

ZB 2002: Formal Specification and Development in Z and B

2nd International Conference of B and Z Users
Grenoble, France, January 23-25, 2002
Proceedings

Springer

Volume Editors

Didier Bert
CNRS, Laboratoire LSR, IMAG
681, rue de la Passerelle
38402 Saint Martin d'Hères Cedex, France
E-mail: didier.bert@imag.fr

Jonathan P. Bowen
South Bank University, SCISM, Centre for Applied Fromal Methods
Borough Road, London SE1 0AA, UK
E-mail: jonathan.bowen@sbu.ac.uk

Martin C. Henson
University of Essex, Department of Computer Science
Wivenhoe Park, Colchester CO4 3SQ, UK
E-mail: hensm@essex.ac.uk

Ken Robinson
The University of New South Wales, UNSW
CAESER, The School of Computer Science and Engineering
Sydney NSW 2052, Australia
E-mail: k.robinson@unsw.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

ZB 2002: formal specification and development in Z and B : proceedings /
2nd International Conference of B and Z Users, Grenoble, France, January
23 - 25, 2002. Didier Bert ... (ed.). - Berlin ; Heidelberg ; New York ;
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2272)
ISBN 3-540-43166-7

CR Subject Classification (1998): D.2.1, D.2.2, D.2.4, F.3.1, F.4.2, F.4.3

ISSN 0302-9743
ISBN 3-540-43166-7 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN 10846165 06/3142 5 4 3 2 1 0

Preface

These proceedings record the papers presented at the second International Conference of B and Z Users (ZB 2002), held on 23–25 January 2002 in the city of Grenoble in the heart of the French Alps. This conference built on the success of the first conference in this series, ZB 2000, held at the University of York in the UK. The location of ZB 2002 in Grenoble reflects the important work in the area of formal methods carried out at the *Laboratoire Logiciels Systèmes Réseaux* within the *Institut d'Informatique et Mathématiques Appliquées de Grenoble* (LSR-IMAG), especially involving the B method.

B and Z are two important formal methods that share a common conceptual origin; each are leading approaches applied in industry and academia for the specification and development (using formal refinement) of computer-based systems. At ZB 2002 the B and Z communities were brought together to hold a second joint conference that simultaneously incorporated the 13th International Z User Meeting and the 4th International Conference on the B method. Although organized logistically as an integral event, editorial control of the joint conference remained vested in two separate but cooperating program committees that respectively determined its B and Z content, but in a coordinated manner.

All the submitted papers in these proceedings were peer reviewed by at least three reviewers drawn from the B or Z committee depending on the subject matter of the paper. Reviewing and initial selection were undertaken electronically. The Z committee met at South Bank University in London on 27th September 2001 to determine the final selection of Z papers. The B committee met on the morning of 28th September 2001 at the Conservatoire National des Arts et Métiers (CNAM) in Paris to select B papers. A joint committee meeting was held at the same location in the afternoon to resolve the final paper selection and to draft a program for the conference. Sergiy Vilkomir of the Centre for Applied Formal Methods (CAFM) at South Bank University aided in the local organization of the Z meeting. Véronique Viguié Donzeau-Gouge helped in the organization of the meetings at CNAM.

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. Our invited speakers for ZB 2002 were drawn from Finland, France, and Canada. Ralph-Johan Back, Professor of Computer Science at Åbo Akademi University and Director of the Turku Centre for Computer Science (TUCS) has made important contributions in the development of the refinement calculus, influential and relevant to many formal methods, including B and Z. Pierre Chartier of RATP (Régie Autonome des Transports Parisiens), central in rail transport for Paris, is a leading expert in the industrial application of the B method. Eric C.R. Hehner, Professor of Computer Science at the University of Toronto, has always presented his novel ideas for formal methods using an elegant simplicity.

Besides its formal sessions, the conference included tool demonstrations, exhibitions, and tutorials. In particular, a workshop on *Refinement of Critical Systems: Methods, Tools, and Experience* (RCS 2002) was organized on 22 January 2001 with the support of the EU IST-RTD Project *MATISSE: Methodologies and Associated Technologies for Industrial Strength Systems Engineering*, in association with the ZB 2002 meeting. Other conference sessions included a presentation on the status of the international Z Standard, in its final stages of acceptance. In addition, the International B Conference Steering Committee (APCB) and the Z User Group (ZUG) used the conference as a convenient venue for open meetings intended for those interested in the B and Z communities respectively.

The topics of interest to the conference included: Industrial applications and case studies using Z or 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; Theoretical issues in formal development (e.g., issues in refinement, proof process, or proof validation, etc.); Software testing versus proof-oriented development; Tools supporting tools for the Z notation and the B method; Development by composition of specifications; Validation of assembly of COTS by model-based specification methods; Z and B extensions and/or standardization.

The ZB 2002 conference was jointly initiated by the Z User Group (ZUG) and the International B Conference Steering Committee (APCB). LSR-IMAG provided all local organization and financial backing for the conference. Without the great support from many local staff at LSR-IMAG and others in Grenoble, ZB 2002 would not have been possible. In particular, we would like to thank the Local Committee Chair, Marie-Laure Potet. ZB 2002 was supported by CNRS (Centre National de la Recherche Scientifique), INPG (Institut National Polytechnique de Grenoble), Université Joseph Fourier (Grenoble), and IMAG. ClearSy System Engineering, Gemplus, the Institut National de Recherche sur les Transports et leur Securité (INRETS), and RATP provided sponsorship. We are grateful to all those who contributed to the success of the conference.

On-line information concerning the conference is available under the following Uniform Resource Locator (URL):

`http://www-lsr.imag.fr/zb2002/`

This also provides links to further on-line resources concerning the B method and Z notation.

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

November 2001

Didier Bert
Jonathan Bowen
Martin Henson
Ken Robinson

Program and Organizing Committees

The following people were members of the ZB 2002 Z program committee:

Conference Chair: Jonathan Bowen, South Bank University, London, UK
Program Chair: Martin Henson, University of Essex, UK

Ali Abdallah, South Bank University, London, UK
Rob Arthan, Lemma 1, Reading, UK
Paolo Ciancarini, University of Bologna, Italy
Neville Dean, Anglia Polytechnic University, UK
John Derrick, The University of Kent at Canterbury, UK
Mark d'Inverno, University of Westminster, UK
Wolfgang Grieskamp, Microsoft Research, USA
Henri Habrias, University of Nantes, France
Jonathan Hammond, Praxis Critical Systems, UK
Ian Hayes, University of Queensland, Australia
Jonathan Jacky, University of Washington, USA
Randolph Johnson, National Security Agency, USA
Steve King, University of York, UK
Kevin Lano, Kings College London, UK
Yves Ledru, LSR-IMAG, Grenoble, France
Jean-Francois Monin, France Telecom R&D, France
Fiona Polack, University of York, UK
Norah Power, University of Limerick, Ireland
Steve Reeves, University of Waikato, New Zealand
Mark Saaltink, ORA, Ottawa, Canada
Thomas Santen, Technical University of Berlin, Germany
Graeme Smith, University of Queensland, Australia
Susan Stepney, Logica Cambridge, UK
Sam Valentine, LiveDevices, York, UK
John Wordsworth, The University of Reading, UK

The following served on the ZB 2002 B program committee:

Program Chair: Didier Bert, CNRS, LSR-IMAG, Grenoble, France
Co-chair: Ken Robinson, The University of New South Wales, Australia

Christian Attiogbé, University of Nantes, France
Richard Banach, University of Manchester, UK
Juan Bicarregui, CLRC, Oxfordshire, UK
Pierre Bieber, CERT, Toulouse, France
Egon Börger, University of Pisa, Italy
Michael Butler, University of Southampton, UK
Dominique Cansell, LORIA, University of Metz, France
Pierre Chartier, RATP, Paris, France
Steve Dunne, University of Teesside, UK
Mark Frappier, University of Sherbrooke, Canada
Andy Galloway, University of York, UK
Jacques Julliand, University of Besançon, France
Jean-Louis Lanet, GemPlus Research Lab, France
Brian Matthews, CLRC, Oxfordshire, UK
Luis-Fernando Mejia, Alstom Transport Signalisation, France
Jean-Marc Meynadier, Matra Transport, France
Louis Mussat, DCSSI, France
Marie-Laure Potet, LSR-IMAG, Grenoble, France
Emil Sekerinski, McMaster University, Canada
Bill Stoddart, University of Teesside, UK
Helen Treharne, Royal Holloway, UK
Véronique Viguié Donzeau-Gouge, CNAM, Paris, France
Marina Walden, Åbo Akademi, Finland

The following people helped with the organization of the conference in various capacities:

B submissions:	Ken Robinson, The University of New South Wales Didier Bert, LSR-IMAG, Grenoble
Z submissions:	Martin Henson, University of Essex Sonia Oakden, University of Essex
Invited speakers:	Ken Robinson, The University of New South Wales
Tool demonstrations:	Mark d'Inverno, University of Westminster Yves Ledru, LSR-IMAG, Grenoble
Tutorials:	Henri Habrias, University of Nantes
Proceedings:	Didier Bert, LSR-IMAG, Grenoble
Local committee:	Marie-Laure Potet (chair), LSR-IMAG, Grenoble Pierre Berlioux, Jean-Claude Reynaud

We are especially grateful to the above for their efforts in ensuring the success of the conference.

External Referees

We are grateful to the following people who aided the program committees in the reviewing of papers, providing additional specialist expertise:

Yamine Ait Ameur, ENSAE/Aérospatiale and ONERA-CERT Toulouse, France
Françoise Bellegarde, Université de Franche-Comté, France
Eerke Boiten, The University of Kent at Canterbury, UK
Lilian Burdy, Laboratoire CEDRIC, CNAM, France
Alessandra Cavarra, Oxford University Computing Laboratory, UK
Fabien Combret, GemPlus, France
Axel Dold, University of Ulm, Germany
Benoit Fraikin, University of Sherbrooke, Canada
Lindsay Groves, Victoria University, New Zealand
Paul Howells, University of Westminster, UK
Olga Kouchnarenko, Université de Franche-Comté, France
Leonid Mikhailov, University of Southampton, UK
Pascal Poizat, Université d'Évry, France
Mike Poppleton, Open University, UK
Antoine Requet, GemPlus, France
Hector Ruiz Barradas, Universidad Autónoma Metropolitana de México
Marianne Simonot, Laboratoire CEDRIC, CNAM, France
Carsten Sühl, GMD, Berlin, Germany
Bruno Tatibouet, Université de Franche-Comté, France
Ray Turner, University of Essex, UK
Mark Utting, University of Waikato, New Zealand
Norbert Völker, University of Essex, UK
Jim Woodcock, The University of Kent at Canterbury, UK

Support

ZB 2002 greatly benefited from the support of the following organizations:

CNRS
IMAG
INP Grenoble
Université Joseph Fourier, Grenoble
Ministère français des Affaires Etrangères

and sponsorship from:

ClearSy System Engineering
GemPlus
INRETS
RATP

Table of Contents