Jacques Julliand
Olga Kouchnarenko (Eds.)

B 2007: Formal Specification and Development in B

LNCS 4355

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

Springer

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

Lecture Notes in Computer Science 4355

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

Lecture Notes in Computer Science

For information about Vols. 1–4246

please contact your bookseller or Springer

Vol. 4355: J. Julliand, O. Kouchnarenko (Eds.), B 2007: Formal Specification and Development in B. XIII, 293 pages. 2006.

Vol. 4345: N. Maglaveras, I. Chouvarda, V. Koutkias, R. Brause (Eds.), Biological and Medical Data Analysis. XIII, 496 pages. 2006. (Sublibrary LNBI).

Vol. 4338: P. Kalra, S. Peleg (Eds.), Computer Vision, Graphics and Image Processing. XV, 965 pages. 2006.

Vol. 4337: S. Arun-Kumar, N. Garg (Eds.), FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science. XIII, 430 pages. 2006.

Vol. 4333: U. Reimer, D. Karagiannis (Eds.), Practical Aspects of Knowledge Management. XII, 338 pages. 2006. (Sublibrary LNAI).

Vol. 4331: G. Min, B. Di Martino, L.T. Yang, M. Guo, G. Ruenger (Eds.), Frontiers of High Performance Computing and Networking – ISPA 2006 Workshops. XXXVII, 1141 pages. 2006.

Vol. 4330: M. Guo, L.T. Yang, B. Di Martino, H.P. Zima, J. Dongarra, F. Tang (Eds.), Parallel and Distributed Processing and Applications. XVIII, 953 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4326: S. Göbel, R. Malkewitz, I. Iurgel (Eds.), Technologies for Interactive Digital Storytelling and Entertainment. X, 384 pages. 2006.

Vol. 4325: J. Cao, I. Stojmenovic, X. Jia, S.K. Das (Eds.), Mobile Ad-hoc and Sensor Networks. XIX, 887 pages. 2006.

Vol. 4320: R. Gotzhein, R. Reed (Eds.), System Analysis and Modeling: Language Profiles. X, 229 pages. 2006.

Vol. 4319: L.-W. Chang, W.-N. Lie (Eds.), Advances in Image and Video Technology. XXVI, 1347 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4313: T. Margaria, B. Steffen (Eds.), Leveraging Applications of Formal Methods. IX, 197 pages. 2006.

Vol. 4312: S. Sugimoto, J. Hunter, A. Rauber, A. Morishima (Eds.), Digital Libraries: Achievements, Challenges and Opportunities. XVIII, 571 pages. 2006.

Vol. 4311: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks II. XI, 253 pages. 2006.

Vol. 4309: P. Inverardi, M. Jazayeri (Eds.), Software Engineering Education in the Modern Age. VIII, 207 pages. 2006.

Vol. 4308: S. Chaudhuri, S.R. Das, H.S. Paul, S. Tirthapura (Eds.), Distributed Computing and Networking. XIX, 608 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4306: Y. Avrithis, Y. Kompatsiaris, S. Staab, N.E. O'Connor (Eds.), Semantic Multimedia. XII, 241 pages. 2006.

Vol. 4305: A.A. Shvartsman (Ed.), Principles of Distributed Systems. XIII, 441 pages. 2006.

Vol. 4304: A. Sattar, B.-H. Kang (Eds.), AI 2006: Advances in Artificial Intelligence. XXVII, 1303 pages. 2006. (Sublibrary LNAI).

Vol. 4302: J. Domingo-Ferrer, L. Franconi (Eds.), Privacy in Statistical Databases. XI, 383 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4297: Y. Robert, M. Parashar, R. Badrinath, V.K. Prasanna (Eds.), High Performance Computing - HiPC 2006. XXIV, 642 pages. 2006.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4295: J.D. Carswell, T. Tezuka (Eds.), Web and Wireless Geographical Information Systems. XI, 269 pages. 2006.

Vol. 4294: A. Dan, W. Lamersdorf (Eds.), Service-Oriented Computing – ICSOC 2006. XIX, 653 pages. 2006.

Vol. 4293: A. Gelbukh, C.A. Reyes-Garcia (Eds.), MICAI 2006: Advances in Artificial Intelligence. XXVIII, 1232 pages. 2006. (Sublibrary LNAI).

Vol. 4292: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part II. XXXII, 906 pages. 2006.

Vol. 4291: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part I. XXXI, 916 pages. 2006.

Vol. 4290: M. van Steen, M. Henning (Eds.), Middleware 2006. XIII, 425 pages. 2006.

Vol. 4289: M. Ackermann, B. Berendt, M. Grobelnik, A. Hotho, D. Mladenič, G. Semeraro, M. Spiliopoulou, G. Stumme, V. Svatek, M. van Someren (Eds.), Semantics, Web and Mining. X, 197 pages. 2006. (Sublibrary LNAI).

Vol. 4288: T. Asano (Ed.), Algorithms and Computation. XX, 766 pages. 2006.

Vol. 4286: P. Spirakis, M. Mavronicolas, S. Kontogiannis (Eds.), Internet and Network Economics. XI, 401 pages. 2006.

Vol. 4285: Y. Matsumoto, R. Sproat, K.-F. Wong, M. Zhang (Eds.), Computer Processing of Oriental Languages. XVII, 544 pages. 2006. (Sublibrary LNAI).

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4282: Z. Pan, A.D. Cheok, M. Haller, R.W.H. Lau, H. Saito, R. Liang (Eds.), Advances in Artificial Reality and Tele-Existence. XXIII, 1347 pages. 2006.

Vol. 4281: K. Barkaoui, A. Cavalcanti, A. Cerone (Eds.), Theoretical Aspects of Computing - ICTAC 2006. XV, 371 pages. 2006.

Vol. 4280: A.K. Datta, M. Gradinariu (Eds.), Stabilization, Safety, and Security of Distributed Systems. XVII, 590 pages. 2006.

Vol. 4279: N. Kobayashi (Ed.), Programming Languages and Systems. XI, 423 pages. 2006.

Vol. 4278: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part II. XLV, 1004 pages. 2006.

Vol. 4277: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part I. XLV, 1009 pages. 2006.

Vol. 4276: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part II. XXXII, 752 pages. 2006.

Vol. 4275: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part I. XXXI, 1115 pages. 2006.

Vol. 4274: Q. Huo, B. Ma, E.-S. Chng, H. Li (Eds.), Chinese Spoken Language Processing. XXIV, 805 pages. 2006. (Sublibrary LNAI).

Vol. 4273: I. Cruz, S. Decker, D. Allemang, C. Preist, D. Schwabe, P. Mika, M. Uschold, L. Aroyo (Eds.), The Semantic Web - ISWC 2006. XXIV, 1001 pages. 2006.

Vol. 4272: P. Havinga, M. Lijding, N. Meratnia, M. Wegdam (Eds.), Smart Sensing and Context. XI, 267 pages. 2006.

Vol. 4271: F.V. Fomin (Ed.), Graph-Theoretic Concepts in Computer Science. XIII, 358 pages. 2006.

Vol. 4270: H. Zha, Z. Pan, H. Thwaites, A.C. Addison, M. Forte (Eds.), Interactive Technologies and Sociotechnical Systems. XVI, 547 pages. 2006.

Vol. 4269: R. State, S. van der Meer, D. O'Sullivan, T. Pfeifer (Eds.), Large Scale Management of Distributed Systems. XIII, 282 pages. 2006.

Vol. 4268: G. Parr, D. Malone, M. Ó Foghlú (Eds.), Autonomic Principles of IP Operations and Management. XIII, 237 pages. 2006.

Vol. 4267: A. Helmy, B. Jennings, L. Murphy, T. Pfeifer (Eds.), Autonomic Management of Mobile Multimedia Services. XIII, 257 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4265: L. Todorovski, N. Lavrač, K.P. Jantke (Eds.), Discovery Science. XIV, 384 pages. 2006. (Sublibrary LNAI).

Vol. 4264: J.L. Balcázar, P.M. Long, F. Stephan (Eds.), Algorithmic Learning Theory. XIII, 393 pages. 2006. (Sublibrary LNAI).

Vol. 4263: A. Levi, E. Savaş, H. Yenigün, S. Balcısoy, Y. Saygın (Eds.), Computer and Information Sciences – ISCIS 2006. XXIII, 1084 pages. 2006.

Vol. 4262: K. Havelund, M. Núñez, G. Roşu, B. Wolff (Eds.), Formal Approaches to Software Testing and Runtime Verification. VIII, 255 pages. 2006.

Vol. 4261: Y. Zhuang, S. Yang, Y. Rui, Q. He (Eds.), Advances in Multimedia Information Processing - PCM 2006. XXII, 1040 pages. 2006.

Vol. 4260: Z. Liu, J. He (Eds.), Formal Methods and Software Engineering. XII, 778 pages. 2006.

Vol. 4259: S. Greco, Y. Hata, S. Hirano, M. Inuiguchi, S. Miyamoto, H.S. Nguyen, R. Słowiński (Eds.), Rough Sets and Current Trends in Computing. XXII, 951 pages. 2006. (Sublibrary LNAI).

Vol. 4257: I. Richardson, P. Runeson, R. Messnarz (Eds.), Software Process Improvement. XI, 219 pages. 2006.

Vol. 4256: L. Feng, G. Wang, C. Zeng, R. Huang (Eds.), Web Information Systems – WISE 2006 Workshops. XIV, 320 pages. 2006.

Vol. 4255: K. Aberer, Z. Peng, E.A. Rundensteiner, Y. Zhang, X. Li (Eds.), Web Information Systems – WISE 2006. XIV, 563 pages. 2006.

Vol. 4254: T. Grust, H. Höpfner, A. Illarramendi, S. Jablonski, M. Mesiti, S. Müller, P.-L. Patranjan, K.-U. Sattler, M. Spiliopoulou, J. Wijsen (Eds.), Current Trends in Database Technology – EDBT 2006. XXXI, 932 pages. 2006.

Vol. 4253: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. XXXII, 1301 pages. 2006. (Sublibrary LNAI).

Vol. 4252: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. XXXIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4251: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXVI, 1297 pages. 2006. (Sublibrary LNAI).

Vol. 4250: H.J. van den Herik, S.-C. Hsu, T.-s. Hsu, H.H.L.M. Donkers (Eds.), Advances in Computer Games. XIV, 273 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4248: S. Staab, V. Svátek (Eds.), Managing Knowledge in a World of Networks. XIV, 400 pages. 2006. (Sublibrary LNAI).

Vol. 4247: T.-D. Wang, X. Li, S.-H. Chen, X. Wang, H. Abbass, H. Iba, G. Chen, X. Yao (Eds.), Simulated Evolution and Learning. XXI, 940 pages. 2006.

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

E-Voting and the Need for Rigourous Software Engineering – The Past, Present and Future

J. Paul Gibson

Department of Computer Science,
National University of Ireland, Maynooth,
Ireland
pgibson@cs.nuim.ie

Abstract. In many jurisdictions around the world, the introduction of e-voting has been subject to wide-ranging debate amongst voters, politicians, political scientists, computer scientists and software engineers. A central issue is one of public trust and confidence: should voters be expected to put their faith in "closed" electronic systems where previously they trusted "open" manual systems?

As the media continues to report on the "failure" of e-voting machines, electoral administrators and e-voting machine manufacturers have been required to review their policies and systems in order to meet a set of ever changing requirements. Such an unstable problem domain stretches their understanding of the electoral process and their ability to apply a diverse range of technologies in providing acceptable electronic solutions. The breadth and depth of the issues suggest that no electoral administration can justifiably claim to have implemented a "trustworthy" electronic replacement for a paper system.

All e-voting systems rely substantially on the correct functioning of their software. It has been argued that such e-voting software is "critical" to its users, and so one would expect to see the highest standards being applied in the development of software in e-voting machines: this is certainly not the case for machines that have already been used. Furthermore, in jurisdictions where e-voting machines have just been procurred we shall see that the software in these machines is often of very poor "quality", even though it has been independently tested and accredited for use.

Throughout the presentation we will focus on the software engineering issues, and will consider the question of whether the formal methods community could have done more - and should do more - to help alleviate the costly problems that society is facing from badly developed software in a wide range of critical government information systems (and not just voting machines).

J. Julliand and O. Kouchnarenko (Eds.): B 2007, LNCS 4355, p. 1, 2006.

Using B Machines for Model-Based Testing of Smartcard Software

Eddie Jaffuel

LEIRIOS Technologies
TEMIS Innovation - 18 Rue Alain Savary - 25000 Besançon, France
eddie.jaffuel@leirios.com
http://www.leirios.com

Abstract. Automated test generation from B abstract machines is commonly used in the smart card industry since 2003. Several domains are concerned such as mobile communication applications (e.g. SIM cards) [1], identity applications (e.g. health cards or identity cards) and banking applications. The model-based testing tool LTG (LEIRIOS Test Generator) [2] makes it possible to generate executable test scripts from a B formal model of the functional requirements. Therefore, the design of the test cases and the development of the test scripts are based on a modeling and automated test generation approach.

The model-based testing process is structured in 3 main steps:

Model. The first step consists in developing a behavior model using the B abstract machine notation. The model represents the expected behavior of the smart card application under test.

Configure test generation. The configuration of the test generation with LTG is based on model coverage criteria. Three families of criteria give a precise control over the test generation: decision coverage, operation effect coverage and data coverage.

Adapt. The generated test cases are then translated in executable test scripts using an adaptor customized for the test execution environment and the project.

This talk show how B abstract machines are developed in the context of model-based testing of smart card applications, how model coverage criteria makes it possible to generate accurate test cases and how those test cases are adapted into executable test scripts for a targeted test execution environment.

References

[1] E. Bernard, B. Legeard, X. Luck, and F. Peureux. Generation of test sequences from formal specifications: GSM 11-11 standard case study. *International Journal of Software Practice and Experience*, 34(10):915–948, 2004.

[2] M. Utting and B. Legeard. *Practical Model-Based Testing - A Tools Approach.* Morgan & Kauffman - Elsevier Science 2006. 528 pages, ISBN 0-12-372501-1.

J. Julliand and O. Kouchnarenko (Eds.): B 2007, LNCS 4355, p. 2, 2006.

The Design of Spacecraft On-Board Software

David Chemouil

French Space Agency (CNES)

Abstract. This presentation deals with the way Space Systems and particularly Spacecraft On-Board Software are designed. I will try to show how the design of Space Systems is undergoing a shift from a seasoned-expert craft to a methodology based upon modelling. First, I will introduce Space Systems by presenting their applications and architecture. Then I will detail the design of such systems, insisting on systems and software aspects. Finally, I will describe some directions currently followed by CNES regarding modelling technologies. Among them, I will bring the notion of pre-proven business-specific refinement patterns to the forefront, as a possible (partial) solution to the reluctance to proof-based development methods in industry.

David Chemouil works in the On-Board Software Office at the French Space Agency (CNES) in Toulouse. His activities include monitoring the development of On-Board Software contracted by CNES and carrying out R&D on Embedded Software Engineering. David Chemouil holds a PhD in Computer Science from Université Paul Sabatier, Toulouse (2004).

J. Julliand and O. Kouchnarenko (Eds.): B 2007, LNCS 4355, p. 3, 2006.