Andrea Bondavalli
Francisco Brasileiro
Sergio Rajsbaum (Eds.)

LNCS 4746

Dependable Computing

Third Latin-American Symposium, LADC 2007
Morelia, Mexico, September 2007
Proceedings

Springer

Andrea Bondavalli Francisco Brasileiro
Sergio Rajsbaum (Eds.)

Dependable Computing

Third Latin-American Symposium, LADC 2007
Morelia, Mexico, September 26-28, 2007
Proceedings

Springer

Volume Editors

Andrea Bondavalli
Università di Firenze, DSI
Viale Morgagni 65, 50134 Firenze, Italy
E-mail: bondavalli@unifi.it

Francisco Brasileiro
Universidade Federal de Campina Grande
Departamento de Sistemas e Computação, Laboratório de Sistemas Distribuídos
Av. Aprígio Veloso, 882 - 58.109-970, Campina Grande, PB, Brazil
E-mail: fubica@dsc.ufcg.edu.br

Sergio Rajsbaum
Universidad Nacional Autónoma de México (UNAM), Instituto de Matemáticas
Ciudad Univesitaria, D.F. 04510, México
E-mail: rajsbaum@math.unam.mx

Library of Congress Control Number: Applied for

CR Subject Classification (1998): C.3, C.4, B.1.3, B.2.3, B.3.4, B.4.5, D.2.4, D.2.8, D.4.5, E.4, J.7

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-75293-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-75293-6 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12167449 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4746

Foreword

The Latin-American Symposium on Dependable Computing, LADC, is the main Latin-American event dedicated to the discussion of the many issues related to dependability in computer systems and networks. It is a forum for researchers and practitioners from all over the world to present and discuss their latest results and experiences in this field. LADC 2007, the third edition of this event, followed on the success of LADC 2005, which took place in Salvador, Bahia, Brazil, and LADC 2003, which took place at the Polytechnic School of the University of São Paulo.

LADC 2007 was co-located with the Mexican Annual Computing Conference (ENC), and AdHoc NOW 2007. It was organized by Universidad Autónoma Metropolitana (UAM) and Universidad Nacional Autónoma de México (UNAM). It was co-sponsored by the Brazilian Computer Society (SBC), the Mexican Society for Computer Science (SMCC), and IEEE TC on Dependable Computing and Fault Tolerance. It was organized in cooperation with IFIP Working Group 10.4 'Dependable Computing and Fault Tolerance,' the Chilean Computer Science Society (SCCC), and the Argentine Society for Informatics and Operations Research (SADIO). LADC 2007 included the following activities:

- Five Technical sessions: Fault-Tolerant Algorithms, Software Engineering of Dependable Systems, Networking and Mobile Computing, Experimental Dependability Evaluation, Intrusion Tolerance and Security
- Two keynote speeches: Philip Koopman (CMU, USA), Jean Arlat (LAAS-CNRS, France)
- Three tutorials: Lorenzo Alvisi (UT Austin, USA), Eduardo B. Fernandez (FAU, USA), Marco Vieira and Henrique Madeira (U Coimbra, Portugal)
- Two panels, chaired by: Henrique Madeira (U Coimbra, Portugal), Rogério de Lemos (U Kent, UK). The latter was a joint panel with AdHoc NOW 2007.

We would like to thank the LADC 2007 Organizing Committee and the support staff of ENC 2007 for having helped us with the organizational tasks, the Steering Committee for their advice, and the Program Committee Co-chairs for their cooperation. Special thanks go to Rogério de Lemos, who was a source of constant support and suggestions. Additionally, we would like to thank the invited guests, all the authors of submitted papers, the sponsoring partners, and Springer for accepting to publish the LADC proceedings in the LNCS series.

We hope all present at LADC 2007 enjoyed the symposium and their stay in Morelia.

September 2007

Sergio Rajsbaum

Preface

The Latin-American Dependable Computing Conference is in its third edition. LADC is the major Latin-American event dedicated to discussing the many issues related to computer system dependability. This symposium succeeded the well-established Brazilian Symposium on Fault-Tolerant Computers. Its objective is to provide a forum for international and Latin-American scientists and engineers to present their latest research results and application experience in this very dynamic field. The first LADC was held in São Paulo, Brazil, in October 2003, while the second was held in Salvador, Brazil, in October 2005. In its third edition the symposium took place in Morelia, Mexico.

This edition of LADC was co-organized by the Universidad Nacional Autónoma de México (UNAM) and the Universidad Autónoma Metropolitana (UAM). It was co-sponsored by SBC—Brazilian Computer Society, SMCC—Mexican Society for Computer Science, and IEEE TC on Dependable Computing and Fault Tolerance. Furthermore, committees of several global professional organizations, such as IFIP Working Group 10.4 'Dependable Computing and Fault-Tolerance', SCCC—Chilean Computer Science Society and SADIO—Argentine Society for Informatics and Operations Research, supported the symposium. LADC is thus the forum for Latin-American researchers in dependability and is extending towards a world-wide dimension as researchers from all over the world show their interest by choosing LADC to submit their manuscripts and present their work.

The selection process was very careful. Each manuscript was sent out for review to three PC members plus two external reviewers. Thirty-seven submissions from 17 countries were received and the 32 members of the Program Committee and 29 external reviewers returned on time a total of 150 reviews. This made the selection process very comprehensive. The committee met in cyberspace to arrange the technical program. A total of 14 papers were selected to appear in the proceedings. The rest of the technical program was defined to include two panels, a forum for 'Fast Abstracts' to report on very recent work and two invited talks by two distinguished scholars: Phil Koopman and Jean Arlat.

We would like to thank the Program Committee members for their help in putting together the final program. They helped us in many ways, right from the beginning, including topic identification, suggestion of external reviewers, refereeing and attending the virtual PC meeting in large numbers. We also thank all of the external reviewers for making available their time and their technical knowledge and the authors of all the manuscripts for their contributions and the timely submissions. Special thanks go to Sergio Rajsbaum, LADC 2007 General Chair, Fabíola Greve, the Fast Abstract Chair, Rogério de Lemos, and Henrique

Madeira, who took leadership in organizing two panels. Finally, we would like to acknowledge the support of the Steering Committee.

We hope you find these conference Proceedings interesting and stimulating.

September 2007

Andrea Bondavalli
Francisco Brasileiro

Organizing Committee

General Chair	Sergio Rajsbaum (Universidad Nacional Autónoma de México, Mexico)
Program Co-chairs	Andrea Bondavalli (Università degli Studi di Firenze, Italy) Francisco Brasileiro (Universidade Federal de Campina Grande, Brazil)
Publication Co-chairs	Fernando Luís Dotti (Pontifícia Universidade Católica do Rio Grande do Sul, Brazil) Imelda Paredes (Universidad Nacional Autónoma de México, Mexico)
Publicity Chair	Fernando Pedone (University of Lugano, Switzerland)
Finance Chair	Elizabeth Pérez (Universidad Autónoma Metropolitana, Mexico)
Local Arrangements Chair	Ricardo Marcelin-Jiménez (Universidad Autónoma Metropolitana, Mexico)
Tutorials Chair	Marcos K. Aguilera (HP Labs,USA)
Fast Abstracts Chair	Fabíola Greve (Universidade Federal da Bahia, Brazil)

Steering Committee

Carlos Maziero	Pontifícia Universidade Católica do Paraná, Brazil
Fabiola Greve	Universidade Federal da Bahia, Brazil
Jean Arlat	Laboratoire d'Analyse et d'Architecture des Systèmes-Centre National de la Recherche Scientifique, France
João Gabriel Silva	Universidade de Coimbra, Portugal
Rogério de Lemos	University of Kent, UK
Sergio Rajsbaum	Universidad Nacional Autónoma de México, Mexico
Taisy Silva Weber (Chair)	Universidade Federal do Rio Grande do Sul, Brazil

LADC Program Committee

Jean Arlat	Laboratoire d'Analyse et d'Architecture des Systèmes - Centre National de la Recherche Scientifique, France
Saurabh Bagchi	Purdue University, USA
Hector Cancela	Universidad de la República, Uruguay
Jose Contreras	Universidad Técnica Federico Santa María, Chile
Bojan Cukic	West Virginia University, USA
Pedro D'Argenio	Universidad Nacional de Córdoba, Argentina
Xavier Defago	Japan Advanced Institute of Science and Technology, Japan
Elias Procópio Duarte Jr.	Universidade Federal do Paraná, Brazil
Christof Fetzer	Technische Universität Dresden, Germany
Joni Fraga	Universidade Federal de Santa Catarina, Brazil
Roy Friedman	Technion - Israel Institute of Technology, Israel
Fabíola Greve	Universidade Federal da Bahia, Brazil
Farnam Jahanian	University of Michigan, USA
Ingrid Jansch-Pôrto	Universidade Federal do Rio Grande do Sul, Brazil
Ricardo Jimenez-Peris	Universidad Politécnica de Madrid, Spain
Henrique Madeira	Universidade de Coimbra, Portugal
Ricardo Marcelín-Jiménez	Universidad Autónoma Metropolitana, Mexico
Magnos Martinello	Fundação Instituto Capixaba de Pesquisas em Contabilidade, Economia e Finanças, Brazil
Eliane Martins	Universidade Estadual de Campinas, Brazil
Keith Marzullo	University of California, San Diego, USA
Carlos Maziero	Pontifícia Universidade Católica do Paraná, Brazil
Pedro Mejia-Alvarez	Instituto Politécnico Nacional, Mexico
Takashi Nanya	University of Tokyo, Japan
Edgar Nett	Otto-von-Guericke-Universität Magdeburg, Germany
Rui Oliveira	Universidade do Minho, Portugal
William Sanders	University of Illinois at Urbana Champaign, USA
André Schiper	Ecole Polytechnique Federale de Lausanne, Switzerland
Richard Schlichting	AT&T Research, USA
Jie Xu	Leeds University, UK
Avelino Zorzo	Pontifícia Universidade Católica do Rio Grande do Sul, Brazil

LADC Referees

Araceli Acosta
Nazareno Aguirre
Pedro Mejia-Alvarez
Jean Arlat
Saurabh Bagchi
Andrea Bondavalli
Francisco Brasileiro
Alcides Calsavara
Hector Cancela
Silvano Chiaradonna
Walfredo Cirne
Victor Costa
Bojan Cukic
Alessandro Daidone
Pedro D'Argenio
Xavier Defago
Felicita Di Giandomenico
Elias Procópio Duarte Jr.
João Durães
Lorenzo Falai
Christof Fetzer
Pablo Florentino
Mauro Fonseca
Joni da Silva Fraga
Roy Friedman
Fabíola Greve
Farnam Jahanian
Ingrid Jansch-Pôrto
Ricardo Jimenez-Peris
Piotr Karwaczynski
Luiz Lento
Paolo Lollini
Pablo Martinez Lopez
Lau Lung
Henrique Madeira
Paulo Mafra
José Maldonado
Ricardo Marcelín-Jiménez
Magnos Martinello
Eliane Martins
Carlos Maziero
Wagner Meira Jr.
Takashi Nanya
Edgar Nett
Rafael Obelheiro
Rui Oliveira
Manoel Camillo de O. Penna Neto
David Powell
José Ferreira de Rezende
Luigi Romano
Jacques Sauvé
André Schiper
Richard Schlichting
Ana Paula da Silva
Neeraj Suri
Andre Gustavo Degraf Uchoa
Nicolas Wolovick
Avelino Zorzo

Co-organizers

Universidad Nacional Autónoma de México (UNAM)
Universidad Autónoma Metropolitana (UAM)

Co-sponsors

SBC—Brazilian Computer Society
SMCC—Mexican Society for Computer Science
IEEE TC on Dependable Computing and Fault Tolerance

In Co-operation with

IFIP Working Group 10.4 'Dependable Computing and Fault-Tolerance'
SCCC—Chilean Computer Science Society
SADIO—Argentine Society for Informatics and Operations Research

Lecture Notes in Computer Science

Sublibrary 1: Theoretical Computer Science and General Issues

For information about Vols. 1–4446
please contact your bookseller or Springer

Vol. 4770: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing. XIII, 460 pages. 2007.

Vol. 4746: A. Bondavalli, F. Brasileiro, S. Rajsbaum (Eds.), Dependable Computing. XIV, 239 pages. 2007.

Vol. 4743: P. Thulasiraman, X. He, T.L. Xu, M.K. Denko, R.K. Thulasiram, L.T. Yang (Eds.), Frontiers of High Performance Computing and Networking ISPA 2007 Workshops. XXIX, 536 pages. 2007.

Vol. 4742: I. Stojmenovic, R.K. Thulasiram, L.T. Yang, W. Jia, M. Guo, R.F. de Mello (Eds.), Parallel and Distributed Processing and Applications. XX, 995 pages. 2007.

Vol. 4736: S. Winter, M. Duckham, L. Kulik, B. Kuipers (Eds.), Spatial Information Theory. XV, 455 pages. 2007.

Vol. 4732: K. Schneider, J. Brandt (Eds.), Theorem Proving in Higher Order Logics. IX, 401 pages. 2007.

Vol. 4731: A. Pelc (Ed.), Distributed Computing. XVI, 510 pages. 2007.

Vol. 4711: C.B. Jones, Z. Liu, J. Woodcock (Eds.), Theoretical Aspects of Computing – ICTAC 2007. XI, 483 pages. 2007.

Vol. 4710: C.W. George, Z. Liu, J. Woodcock (Eds.), Domain Modeling and the Duration Calculus. XI, 237 pages. 2007.

Vol. 4708: L. Kučera, A. Kučera (Eds.), Mathematical Foundations of Computer Science 2007. XVIII, 764 pages. 2007.

Vol. 4707: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part III. XXIV, 1205 pages. 2007.

Vol. 4706: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part II. XXIII, 1129 pages. 2007.

Vol. 4705: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part I. XLIV, 1169 pages. 2007.

Vol. 4703: L. Caires, V.T. Vasconcelos (Eds.), CONCUR 2007 – Concurrency Theory. XIII, 507 pages. 2007.

Vol. 4700: C.B. Jones, Z. Liu, J. Woodcock (Eds.), Formal Methods and Hybrid Real-Time Systems. XVI, 539 pages. 2007.

Vol. 4697: L. Choi, Y. Paek, S. Cho (Eds.), Advances in Computer Systems Architecture. XIII, 400 pages. 2007.

Vol. 4688: K. Li, M. Fei, G.W. Irwin, S. Ma (Eds.), Bio-Inspired Computational Intelligence and Applications. XIX, 805 pages. 2007.

Vol. 4684: L. Kang, Y. Liu, S. Zeng (Eds.), Evolvable Systems: From Biology to Hardware. XIV, 446 pages. 2007.

Vol. 4683: L. Kang, Y. Liu, S. Zeng (Eds.), Intelligence Computation and Applications. XVII, 663 pages. 2007.

Vol. 4681: D.-S. Huang, L. Heutte, M. Loog (Eds.), Advanced Intelligent Computing Theories and Applications. XXVI, 1379 pages. 2007.

Vol. 4672: K. Li, C. Jesshope, H. Jin, J.-L. Gaudiot (Eds.), Network and Parallel Computing. XVIII, 558 pages. 2007.

Vol. 4671: V. Malyshkin (Ed.), Parallel Computing Technologies. XIV, 635 pages. 2007.

Vol. 4669: J.M. de Sá, L.A. Alexandre, W. Duch, D. Mandic (Eds.), Artificial Neural Networks – ICANN 2007, Part II. XXXI, 990 pages. 2007.

Vol. 4668: J.M. de Sá, L.A. Alexandre, W. Duch, D. Mandic (Eds.), Artificial Neural Networks – ICANN 2007, Part I. XXXI, 978 pages. 2007.

Vol. 4666: M.E. Davies, C.J. James, S.A. Abdallah, M.D Plumbley (Eds.), Independent Component Analysis and Blind Signal Separation. XIX, 847 pages. 2007.

Vol. 4665: J. Hromkovič, R. Královič, M. Nunkesser, P. Widmayer (Eds.), Stochastic Algorithms: Foundations and Applications. X, 167 pages. 2007.

Vol. 4664: J. Durand-Lose, M. Margenstern (Eds.), Machines, Computations, and Universality. X, 325 pages. 2007.

Vol. 4649: V. Diekert, M.V. Volkov, A. Voronkov (Eds.), Computer Science – Theory and Applications. XIII, 420 pages. 2007.

Vol. 4647: R. Martin, M. Sabin, J. Winkler (Eds.), Mathematics of Surfaces XII. IX, 509 pages. 2007.

Vol. 4646: J. Duparc, T.A. Henzinger (Eds.), Computer Science Logic. XIV, 600 pages. 2007.

Vol. 4644: N. Azémard, L. Svensson (Eds.), Integrated Circuit and System Design. XIV, 583 pages. 2007.

Vol. 4641: A.-M. Kermarrec, L. Bougé, T. Priol (Eds.), Euro-Par 2007 Parallel Processing. XXVII, 974 pages. 2007.

Vol. 4639: E. Csuhaj-Varjú, Z. Ésik (Eds.), Fundamentals of Computation Theory. XIV, 508 pages. 2007.

Vol. 4638: T. Stützle, M. Birattari, H. H. Hoos (Eds.), Engineering Stochastic Local Search Algorithms. X, 223 pages. 2007.

Vol. 4628: L.N. de Castro, F.J. Von Zuben, H. Knidel (Eds.), Artificial Immune Systems. XII, 438 pages. 2007.

Vol. 4627: M. Charikar, K. Jansen, O. Reingold, J.D.P. Rolim (Eds.), Approximation, Randomization, and Combinatorial Optimization. XII, 626 pages. 2007.

Vol. 4624: T. Mossakowski, U. Montanari, M. Haveraaen (Eds.), Algebra and Coalgebra in Computer Science. XI, 463 pages. 2007.

Vol. 4621: D. Wagner, R. Wattenhofer (Eds.), Algorithms for Sensor and Ad Hoc Networks. XIII, 415 pages. 2007.

Vol. 4619: F. Dehne, J.-R. Sack, N. Zeh (Eds.), Algorithms and Data Structures. XVI, 662 pages. 2007.

Vol. 4618: S.G. Akl, C.S. Calude, M.J. Dinneen, G. Rozenberg, H.T. Wareham (Eds.), Unconventional Computation. X, 243 pages. 2007.

Vol. 4616: A. Dress, Y. Xu, B. Zhu (Eds.), Combinatorial Optimization and Applications. XI, 390 pages. 2007.

Vol. 4613: F.P. Preparata, Q. Fang (Eds.), Frontiers in Algorithmics. XI, 348 pages. 2007.

Vol. 4600: H. Comon-Lundh, C. Kirchner, H. Kirchner (Eds.), Rewriting, Computation and Proof. XVI, 273 pages. 2007.

Vol. 4599: S. Vassiliadis, M. Berekovic, T.D. Hämäläinen (Eds.), Embedded Computer Systems: Architectures, Modeling, and Simulation. XVIII, 466 pages. 2007.

Vol. 4598: G. Lin (Ed.), Computing and Combinatorics. XII, 570 pages. 2007.

Vol. 4596: L. Arge, C. Cachin, T. Jurdziński, A. Tarlecki (Eds.), Automata, Languages and Programming. XVII, 953 pages. 2007.

Vol. 4595: D. Bošnački, S. Edelkamp (Eds.), Model Checking Software. X, 285 pages. 2007.

Vol. 4590: W. Damm, H. Hermanns (Eds.), Computer Aided Verification. XV, 562 pages. 2007.

Vol. 4588: T. Harju, J. Karhumäki, A. Lepistö (Eds.), Developments in Language Theory. XI, 423 pages. 2007.

Vol. 4583: S.R. Della Rocca (Ed.), Typed Lambda Calculi and Applications. X, 397 pages. 2007.

Vol. 4580: B. Ma, K. Zhang (Eds.), Combinatorial Pattern Matching. XII, 366 pages. 2007.

Vol. 4576: D. Leivant, R. de Queiroz (Eds.), Logic, Language, Information and Computation. X, 363 pages. 2007.

Vol. 4547: C. Carlet, B. Sunar (Eds.), Arithmetic of Finite Fields. XI, 355 pages. 2007.

Vol. 4546: J. Kleijn, A. Yakovlev (Eds.), Petri Nets and Other Models of Concurrency – ICATPN 2007. XI, 515 pages. 2007.

Vol. 4545: H. Anai, K. Horimoto, T. Kutsia (Eds.), Algebraic Biology. XIII, 379 pages. 2007.

Vol. 4533: F. Baader (Ed.), Term Rewriting and Applications. XII, 419 pages. 2007.

Vol. 4528: J. Mira, J.R. Álvarez (Eds.), Nature Inspired Problem-Solving Methods in Knowledge Engineering, Part II. XXII, 650 pages. 2007.

Vol. 4527: J. Mira, J.R. Álvarez (Eds.), Bio-inspired Modeling of Cognitive Tasks, Part I. XXII, 630 pages. 2007.

Vol. 4525: C. Demetrescu (Ed.), Experimental Algorithms. XIII, 448 pages. 2007.

Vol. 4514: S.N. Artemov, A. Nerode (Eds.), Logical Foundations of Computer Science. XI, 513 pages. 2007.

Vol. 4513: M. Fischetti, D.P. Williamson (Eds.), Integer Programming and Combinatorial Optimization. IX, 500 pages. 2007.

Vol. 4510: P. Van Hentenryck, L.A. Wolsey (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 391 pages. 2007.

Vol. 4507: F. Sandoval, A.G. Prieto, J. Cabestany, M. Graña (Eds.), Computational and Ambient Intelligence. XXVI, 1167 pages. 2007.

Vol. 4501: J. Marques-Silva, K.A. Sakallah (Eds.), Theory and Applications of Satisfiability Testing – SAT 2007. XI, 384 pages. 2007.

Vol. 4497: S.B. Cooper, B. Löwe, A. Sorbi (Eds.), Computation and Logic in the Real World. XVIII, 826 pages. 2007.

Vol. 4494: H. Jin, O.F. Rana, Y. Pan, V.K. Prasanna (Eds.), Algorithms and Architectures for Parallel Processing. XIV, 508 pages. 2007.

Vol. 4493: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part III. XXVI, 1215 pages. 2007.

Vol. 4492: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part II. XXVII, 1321 pages. 2007.

Vol. 4491: D. Liu, S. Fei, Z.-G. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part I. LIV, 1365 pages. 2007.

Vol. 4490: Y. Shi, G.D. van Albada, J.J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part IV. XXXVII, 1211 pages. 2007.

Vol. 4489: Y. Shi, G.D. van Albada, J.J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part III. XXXVII, 1257 pages. 2007.

Vol. 4488: Y. Shi, G.D. van Albada, J.J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part II. XXXV, 1251 pages. 2007.

Vol. 4487: Y. Shi, G.D. van Albada, J.J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part I. LXXXI, 1275 pages. 2007.

Vol. 4484: J.-Y. Cai, S.B. Cooper, H. Zhu (Eds.), Theory and Applications of Models of Computation. XIII, 772 pages. 2007.

Vol. 4475: P. Crescenzi, G. Prencipe, G. Pucci (Eds.), Fun with Algorithms. X, 273 pages. 2007.

Vol. 4474: G. Prencipe, S. Zaks (Eds.), Structural Information and Communication Complexity. XI, 342 pages. 2007.

Vol. 4459: C. Cérin, K.-C. Li (Eds.), Advances in Grid and Pervasive Computing. XVI, 759 pages. 2007.

Vol. 4449: Z. Horváth, V. Zsók, A. Butterfield (Eds.), Implementation and Application of Functional Languages. X, 271 pages. 2007.

Vol. 4448: M. Giacobini (Ed.), Applications of Evolutionary Computing. XXIII, 755 pages. 2007.

Vol. 4447: E. Marchiori, J.H. Moore, J.C. Rajapakse (Eds.), Evolutionary Computation, Machine Learning and Data Mining in Bioinformatics. XI, 302 pages. 2007.

¥484.00元

Table of Contents

Invited Talks

Fault-Tolerant Algorithms

Software Engineering of Dependable Systems

Networking and Mobile Computing

Experimental Dependability Evaluation

Intrusion Tolerance and Security

Tutorials

Panels

Reliability, Safety, and Security in Everyday Embedded Systems
(Extended Abstract)

Philip Koopman

Carnegie Mellon University
Pittsburgh, PA 15213, USA
koopman@cmu.edu

Embedded systems permeate our everyday lives. From automobiles to elevators, kitchen appliances to televisions, and water heaters to cell phones, we increasingly depend upon embedded systems to operate as expected. A few obviously critical embedded application domains, such as aviation, have traditionally benefited from extraordinary care during development to ensure that everything is done correctly. But increasingly, everyday embedded applications are becoming "mission critical," with little fanfare and perhaps without the full attention to dependability properties that they truly deserve.

Consider the following potentially significant failure modes for embedded systems: A cell phone that doesn't work when the owner needs to call for emergency medical attention. A domestic hot water heater that overheats water, causing scalding burns on a child. A thermostat that doesn't turn on heat when needed, causing household water pipes to freeze and burst. A microwave oven that turns on with the door open. An automobile that unintendedly accelerates. Today, hardware interlocks mitigate many of these hazards. But, software is playing a bigger role as both a vulnerability and a mitigation mechanism for critical failures. Because most embedded systems have actuators that influence the environment, and because people count on them to operate as expected, special care must be taken to ensure that they are safe, reliable, and secure.

Safety in the context of embedded systems deals with minimizing the frequency of mishaps (especially loss of life, injuries, and damage to property). In many ways this is the most mature of the areas we are discussing, because there are several industry-specific standards that can be followed to create safe systems (e.g., IEC 61508). There are, however, some significant research challenges outstanding in this area, including:

- How can we be sure that following a given system development process actually results in the hoped-for level of safety?
- How can we make it easy for small, non-specialist teams of domain experts to follow complex, "heavy-weight" safety standards and actually get it right?
- How can we simplify the representation and specification of safety properties to make it easier to design safe systems?

Reliability in embedded systems has been studied for many years, and has to do with ensuring that once an embedded system starts a "mission," it has a high probability of completing that mission without experiencing a failure. Traditional high-reliability systems have used hardware redundancy (for example, two engines on an airplane instead of one). But, cost-sensitive everyday embedded systems often do not have a price structure that permits redundancy. An even bigger problem is

A. Bondavalli, F. Brasileiro, and S. Rajsbaum (Eds.): LADC 2007, LNCS 4746, pp. 1–2, 2007.

creating highly reliable software, especially with quick time-to-market and low development budget constraints. Some current research challenges in this area are:

- How can we make it easy for small, non-specialist teams of domain experts to create highly reliable software?
- How can we quantify software reliability to support testing for design requirements such as "software crashes no more than once per month"?
- Achieving absolute software perfection seems unrealistic. How can we create embedded systems that survive the activation of latent software defects?

Security is, of course, a hot topic. But currently, it seems to be getting less attention in embedded systems than in enterprise systems. While embedded systems have not yet experienced as many widely publicized security problems as enterprise systems have, the potential for widespread, significant impact to society is certainly there. What happens if malicious attackers gain control of many embedded systems with the ability to release energy (or hazardous substances) into the environment? What if some critical infrastructure, such as energy distribution, traffic flow control, building environmental services, or telecommunications, suddenly stops working? While there are no easy answers to security in any environment, embedded systems present unique challenges that require research beyond the scope of enterprise security research, including:

- How can we make it easy for small, non-specialist teams of domain experts to get security right, even on a small product?
- What unique security challenges arise when interconnecting embedded systems (for example, coordinating actuators across many systems)?
- What novel vulnerabilities arise in Internet-connected embedded systems?
- What security concerns arise due to threats unique to embedded systems (for example, when the system owner is the attacker).

Embedded systems have historically been simple, often non-critical, and usually very reliable, safe, and secure. Newer systems are becoming more complex, and starting to cross the fuzzy line from non-critical to criticality. Unfortunately, the techniques and culture of developers for newly critical applications often do not take into account this major shift. While improving developer literacy in the areas of reliability, safety, and security will help, significant research challenges remain.

A common, underlying challenge has to do with the central role of domain experts in embedded system design. It is common for embedded system development teams to be relatively small, and staffed more with domain experts than computing experts. This is often appropriate, because expert domain knowledge is crucial to success. However, small teams and companies that are concerned mostly with an application domain rather than computer technology often don't have access to expertise in dependability. So, even if researchers can solve the many outstanding research problems, there is still the issue of finding ways to deploy that knowledge to everyday working engineers whose training is often not primarily in computing. We must not only solve the research questions, but also find a way to deploy that knowledge.

This work was supported in part by the General Motors Collaborative Research Center at Carnegie Mellon University.