Lecture Notes in Computer Science 6894

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

Francesco Flammini Sandro Bologna
Valeria Vittorini (Eds.)

Computer Safety, Reliability, and Security

30th International Conference, SAFECOMP 2011
Naples, Italy, September 19-22, 2011
Proceedings

Springer

Volume Editors

Francesco Flammini
Ansaldo STS
Via Argine, 425, 80147 Napoli, Italy
E-mail: francesco.flammini@ansaldo-sts.com

Sandro Bologna
Italian Association Critical Infrastructure (AIIC)
Rome, Italy
E-mail: s.bologna@infrastrutturecritiche.it

Valeria Vittorini
Università di Napoli Federico II
Dipartimento di Informatica e Sistemistica
Via Claudio, 21, 80125 Napoli, Italy
E-mail: valeria.vittorini@unina.it

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-24269-4 e-ISBN 978-3-642-24270-0
DOI 10.1007/978-3-642-24270-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011936469

CR Subject Classification (1998): K.6.5, C.2, D.2, H.3, D.4.6, E.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Some outstanding writers of the last century have depicted an imaginary future in which intelligent machines ruled upon human beings. While most of the machines surrounding us can not be considered "intelligent" in the common sense (though they probably would to the eyes of people of some decades ago), a similar scenario can be considered nowadays as real: we do realize or not, nearly every activity we perform during our everyday life relies upon the dependability of computer-controlled devices, ranging from automatic transaction modules to brake-by-wire systems.

Furthermore, it is a matter of fact that the complexity and criticality of computer systems have grown substantially in the last years, and they are continuously increasing. Complexity is a result of three main factors: size, distribution and heterogeneity. Size refers to the number of functionalities requested to modern computers, which imply larger programs. Distribution is an effect of the need for networked devices, almost always required by the specific applications. Heterogeneity is given by the different hardware and software architectures involved in the design. The criticality attribute is related to the domains in which computer systems operate, whereas a failure can cause a significant loss of money, injuries, kills or even natural disasters. Please note that "critical" does not always imply "hard real-time".

Such a scenario requires the adoption of novel techniques and tools in order to assure the dependability of computer systems, taking into account their interaction with other entities in terms both of the negative effects of the system upon the external environment (safety) and of the external environment upon the system (security).

The idea behind the choice of the main theme of the 30th edition of the International Conference on Computer Safety, Reliability and Security (SAFECOMP 2011) has been the need for mastering complexity and criticality of modern computer-based systems. One of the best way to address that issue is the adoption of rigorous model-based engineering techniques, together with a holistic system-centric view, including all the components, abstraction layers and life-cycle phases.

As a result of this choice, the program of the conference reflects the contributor expertise in the following specialties, which are strictly related to the development of high-assurance systems:

- Computer dependability, studying the dynamics of propagation of random and systematic faults and the related protection mechanisms (fault-tolerance, error management, etc.).
- Software engineering, with special focus on simulative and analytical approaches of verification and validation (including software testing and formal methods).

- Risk analysis, addressing multi-disciplinary aspects of man-machine interaction and safety assessment procedures, using both qualitative and quantitative means.
- Multi-paradigm modeling, needed to master the increasing complexity of critical systems by integrating and evaluating heterogeneous models in cohesive system-level views.
- Information security, which plays an important role in high-integrity and business critical systems, needing robust authentication and communication protocols to protect against natural as well as malicious threats.

Such a mixture of topics has also helped to fill the "gap" existing between the research areas of computer dependability and critical infrastructure security.

All the aforementioned issues are addressed in this book, which represents the proceedings of the 30th edition of the International Conference on Computer Safety, Reliability and Security (SAFECOMP 2011), held in Naples, Italy, 19-21 September 2011. The proceedings includes 34 papers, but the response to the call for Papers was so high, that make all papers could be included in the volume.

As Chairpersons of the International Program Committee (IPC) and the National Organizing Committee, we would like to thank all authors who submitted their work, the presenters of the papers, the members of the IPC, the reviewers, the members of the National Organizing Committee, the session chairmen, and the sponsors for their efforts and support. Without their strong motivation and hard work we could not develop a succesfull and valuable conference as well as this book of proceedings.

September 2011

Francesco Flammini
Sandro Bologna
Roberto Setola
Valeria Vittorini

Organization

SAFECOMP 2001 has been organized by Dipartimento di Informatica e Sistemistica - University of Naples Federico II, Centro Regionale ICT (CeRICT), Ansaldo STS and European Workshop on Industrial Computer Systems Reliability, Safety and Security (EWICS).

EWICS Chair

Francesca Saglietti (University of Erlangen-Nüemberg, Germany)

Honorary Chairs

Giovanni Bocchetti (Ansaldo STS, Italy)
Giorgio Franceschetti (University of Naples Federico II, Italy)
Antonino Mazzeo (University of Naples Federico II, Italy)

Program Chairs

Francesco Flammini (Ansaldo STS, Italy)
Sandro Bologna (ENEA, Italy)

Local Chairs

Nicola Mazzocca (University of Naples Federico II, Italy)
Concetta Pragliola (Ansaldo STS, Italy)
Roberto Setola (University Campus Biomedico of Rome, Italy)
Valeria Vittorini (University of Naples Federico II, Italy)

Program Committee

J.P. Blanquart (FR)
A. Bondavalli (IT)
R. Bloomfield (UK)
B. Buth (DE)
A. Coronato (IT)
D. Cotroneo (IT)
G. D'Agostino (IT)
P. Daniel (UK)
S. DAntonio (IT)
G. De Pietro (IT)
F. Di Giandomenico (IT)
W. Ehrenberger (DE)
M. Felici (UK)
N. Ferreia Neves (PT)
G. Franceschinis (IT)
G. Gigante (IT)
L. Glielmo (IT)
J. Gorski (PL)

W. Halang (DE)
R.E. Harper (USA)
M. Heisel (DE)
J. Jurjens (DE)
R. Jimenez (ES)
K. Kanoun (FR)
J. Karlsson (SE)
T. Kelly (UK)
F. Koornneef (NL)
P. Ladkin (DE)
S. Lindskov Hansen (DK)
B. Littlewood (UK)
G. Manco (IT)
T. Margaria (DE)
E. Meda (IT)
P.J. Mosterman (USA)
T. Nanya (Japan)
O. Nordland (NO)
F. Ortmeier (DE)
A. Pataricza (HU)
D. Powell (FR)
P. Prinetto (IT)
L. Romano (IT)
A. Romanovsky (UK)
S. Russo (IT)
F. Saglietti (DE)
E. Schoitsch (AT)
T. Seyfarth (DE)
B. Siciliano (IT)
L. Strigini (UK)
M. Sujan (UK)
N. Suri (DE)
K. Trivedi (USA)
M. van der Meulen (NL)
V. Vittorini (IT)
A. Vozella (IT)
S. Zanero (IT)
Z. Zurakowski (PL)

Additional Reviewers

Flora Amato (IT)
Fabrizio Baiardi (IT)
Gianmarco Baldini (IT)
Claudio Bareato (CH)
Angelo Berghella (IT)
Simona Bernardi (E)
Andrea Bobbio (IT)
Claudio Luigi Brasca (IT)
Luigi Buonanno (IT)
Audrey Canning (UK)
Emiliano Casalicchio (IT)
Valentina Casola (IT)
Mario Ciampi (IT)
Emanuele Ciapessoni (IT)
Tadeusz Cichocki (PL)
Alessandro Cilardo (IT)
Carlo Alberto Clarotti (IT)
Andrea Colini (IT)
Antonio Di Pietro (IT)
Stelios Dritsas (GR)
Massimo Esposito (IT)
Anna Rita Fasolino (IT)
Andrea Fiaschetti (IT)
Roberto Filippini (IT)
Vincenzo Fioriti (IT)
Chiara Foglietta (IT)
Luisa Franchina (IT)
Giustino Fumagalli (IT)
Andrea Gaglione (IT)
Ilir Gashi (UK)
Gokce Gorbil (UK)
Dimitris Gritzalis (GR)
Vincenzo Gulisano (E)
Mauro Iacono (IT)
Federico Maggi (IT)
Loredana Mancini (IT)
Stefano Marrone (IT)
Fiammetta Marulli (IT)
Francesca Matarese (IT)
Oliver Meyer (DE)
Paolo Nocito (IT)
Gabriele Oliva (IT)
Antonio Orazzo (IT)
Stefano Panzieri (IT)
Alfio Pappalardo (IT)
Peter Popov (UK)

Andrey Povyakalo (UK)
Erich Rome (DE)
Guido Salvaneschi (IT)
Damian Serrano (FR)
Claudio Soriente (E)
Federica Sorrentino (IT)
Luigi Sportiello (IT)
Marianthi Theoharidou (GR)
Alberto Tofani (IT)
Bill Tolone (USA)
Enrico Tronci (IT)
Salvatore Venticinque (IT)
Min Wu (USA)
Christos Xenakis (GR)
Loredana Zollo (IT)

Organizing Committee

Flora Amato	University of Naples Federico II
Carmen C. Baruffini	University of Naples Federico II
Valentina Casola	University of Naples Federico II
Alessandra De Benedictis	University of Naples Federico II
Domenico Di Leo	University of Naples Federico II
Stefano Marrone	Second University of Naples
Roberto Nardone	University of Naples Federico II
Alfio Pappalardo	University of Naples Federico II
Antonio Pecchia	University of Naples Federico II
Sara Romano	University of Naples Federico II

Table of Contents

Session 1: Ram Evaluation 1

Session 2: Complex Systems Dependability 1

Session 3: Formal Verification 1

Session 4: Risk and Hazard Analysis

Session 5: Cybersecurity

Session 6: RAM Evaluation 2

Session 7: Case Studies

Session 8: Formal Verification 2

Poster Session

Session 9: Formal Verification 3

Session 10: Optimization Methods

Session 11: Complex Systems Dependability 2