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
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-Nürnberg, 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)  G. De Pietro (IT)
A. Bondavalli (IT)  F. Di Giandomenico (IT)
R. Bloomfield (UK)  W. Ehrenberger (DE)
B. Buth (DE)  M. Felici (UK)
A. Coronato (IT)  N. Ferreia Neves (PT)
D. Cotroneo (IT)  G. Franceschinis (IT)
G. D’Agostino (IT)  G. Gigante (IT)
P. Daniel (UK)  L. Glielmo (IT)
S. DAntonio (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. Sujuan (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)  
Emmanuele Ciaipessoni (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)  Alberto Tofani (IT)
Erich Rome (DE)  Bill Tolone (USA)
Guido Salvaneschi (IT)  Enrico Tronci (IT)
Damian Serrano (FR)  Salvatore Venticinque (IT)
Claudio Soriente (E)  Min Wu (USA)
Federica Sorrentino (IT)  Christos Xenakis (GR)
Luigi Sportiello (IT)  Loredana Zollo (IT)
Marianthi Theoharidou (GR)

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

The Effect of Correlated Failure Rates on Reliability of Continuous Time 1-Out-of-2 Software ........................................ 1  
*Peter Popov and Gabriele Manno*

Model-Driven Availability Evaluation of Railway Control Systems ...... 15  
*Simona Bernardi, Francesco Flammini, Stefano Marrone, José Merseguer, Camilla Papa, and Valeria Vittorini*

## Session 2: Complex Systems Dependability 1

Vertical Safety Interfaces – Improving the Efficiency of Modular Certification ......................................................... 29  
*Bastian Zimmer, Susanne Bürklen, Michael Knoop, Jens Höflinger, and Mario Trapp*

DALculus – Theory and Tool for Development Assurance Level Allocation ................................................................. 43  
*Pierre Bieber, Rémi Delmas, and Christel Seguin*

*Jean-Paul Blanquart, Eric Armengaud, Philippe Baufreton, Quentin Bourrouilh, Gerhard Griessnig, Martin Krammer, Odile Laurent, Joseph Machrouh, Thomas Peikenkamp, Cecile Schindler, and Tormod Wien*

## Session 3: Formal Verification 1

From Probabilistic Counterexamples via Causality to Fault Trees ...... 71  
*Matthias Kuntz, Florian Leitner-Fischer, and Stefan Leue*

Rigorous Evidence of Freedom from Concurrency Faults in Industrial Control Software ...................................................... 85  
*Richard Bonichon, Géraud Canet, Loïc Correnson, Éric Goubault, Emmanuel Haucourt, Michel Hirschowitz, Sébastien Labbé, and Samuel Mimram*
### Session 4: Risk and Hazard Analysis

**Evolutionary Risk Analysis: Expert Judgement** .......................... 99  
*Massimo Felici, Valentino Meduri, Bjørnar Solhaug, and Alessandra Tedeschi*

**Computer-Aided PHA, FTA and FMEA for Automotive Embedded Systems** ......................................................... 113  
*Roland Mader, Eric Armengaud, Andrea Leitner, Christian Kreiner, Quentin Bourrouilh, Gerhard Grießnig, Christian Steger, and Reinhold Weiβ*

### Session 5: Cybersecurity

**A Statistical Anomaly-Based Algorithm for On-line Fault Detection in Complex Software Critical Systems** ................................................ 128  
*Antonio Bovenzi, Francesco Brancati, Stefano Russo, and Andrea Bondavalli*

**Security Analysis of Smart Grid Data Collection Technologies** ....... 143  
*Luigi Coppolino, Salvatore D’Antonio, Ivano Alessandro Elia, and Luigi Romano*

### Session 6: RAM Evaluation 2

**Modeling Aircraft Operational Reliability** ............................ 157  
*Kossi Tiassou, Karama Kanoun, Mohamed Kaâniche, Christel Seguin, and Chris Papadopoulos*

**An Integrated Approach for Availability and QoS Evaluation in Railway Systems** ................................................................. 171  
*Antonino Mazzeo, Nicola Mazzocca, Roberto Nardone, Luca D’Acierno, Bruno Montella, Vincenzo Punzo, Egidio Quaglietta, Immacolata Lamberti, and Pietro Marmo*

### Session 7: Case Studies

**Using a Software Safety Argument Pattern Catalogue: Two Case Studies** ................................................................. 185  
*Richard Hawkins, Kester Clegg, Rob Alexander, and Tim Kelly*

**Integration of a System for Critical Infrastructure Protection with the OSSIM SIEM Platform: A Dam Case Study** ................................. 199  
*Luigi Coppolino, Salvatore D’Antonio, Valerio Formicola, and Luigi Romano*
A Case Study on State-Based Robustness Testing of an Operating System for the Avionic Domain ........................................ 213
   Domenico Cotroneo, Domenico Di Leo, Roberto Natella, and Roberto Pietrantuono

Session 8: Formal Verification 2

Formal Methods for the Certification of Autonomous Unmanned Aircraft Systems ........................................ 228
   Matt Webster, Michael Fisher, Neil Cameron, and Mike Jump

Verifying Functional Behaviors of Automotive Products in EAST-ADL2 Using UPPAAL-PORT ......................... 243
   Eun-Young Kang, Pierre-Yves Schobbens, and Paul Pettersson

Poster Session

Establishing Confidence in the Usage of Software Tools in Context of ISO 26262 ........................................ 257
   Joachim Hillebrand, Peter Reichenpfader, Irenka Mandic, Hannes Siegl, and Christian Peer

Fault-Based Generation of Test Cases from UML-Models – Approach and Some Experiences ....................... 270
   Rupert Schlick, Wolfgang Herzner, and Elisabeth Jöbstl

ISO/IEC 15504-10: Motivations for Another Safety Standard ........ 284
   Giuseppe Lami, Fabrizio Fabbrini, and Mario Fusani

Automatic Synthesis of SRN Models from System Operation Templates for Availability Analysis ................... 296
   Kumiko Tadano, Jiangwen Xiang, Masahiro Kawato, and Yoshiharu Maeno

A Collaborative Event Processing System for Protection of Critical Infrastructures from Cyber Attacks .............. 310
   Leonardo Aniello, Giuseppe A. Di Luna, Giorgia Lodi, and Roberto Baldoni

A Fault-Tolerant, Dynamically Scheduled Pipeline Structure for Chip Multiprocessors ................................. 324
   Hananeh Ali and Hamid Reza Zarandi

FloGuard: Cost-Aware Systemwide Intrusion Defense via Online Forensics and On-Demand IDS Deployment .... 338
   Saman Aliari Zonouz, Kaustubh R. Joshi, and William H. Sanders
Reducing Complexity of Data Flow Testing in the Verification of a IEC-62304 Flexible Workflow System .................................. 355
Federico Cruciani and Enrico Vicario

Improvement of Processes and Methods in Testing Activities for Safety-Critical Embedded Systems .................................................. 369
Giuseppe Bonifacio, Pietro Marmo, Antonio Orazzo, Ida Petrone,
Luigi Velardi, and Alessio Venticinque

Session 9: Formal Verification 3

On the Adoption of Model Checking in Safety-Related Software Industry .......................................................... 383
Alessandro Fantechi and Stefania Gnesi

Equivalence Checking between Function Block Diagrams and C Programs Using HW-CBMC ........................................... 397
Dong-Ah Lee, Junbeom Yoo, and Jang-Soo Lee

A Framework for Simulation and Symbolic State Space Analysis of Non-Markovian Models ........................................ 409
Laura Carnevali, Lorenzo Ridi, and Enrico Vicario

Session 10: Optimization Methods

Model-Based Multi-objective Safety Optimization ...................... 423
Matthias Güdemann and Frank Ortmeier

Tradeoff Exploration between Reliability, Power Consumption, and Execution Time .......................................................... 437
Ismail Assayad, Alain Girault, and Hamoudi Kalla

Session 11: Complex Systems Dependability 2

Criticality-Driven Component Integration in Complex Software Systems .......................................................... 452
Antonio Pecchia, Roberto Pietrantuono, and Stefano Russo

On the Use of Semantic Technologies to Model and Control Security, Privacy and Dependability in Complex Systems .................. 467
Andrea Fiaschetti, Francesco Lavorato, Vincenzo Suraci,
Andi Palo, Andrea Taglialetela, Andrea Morgagni,
Renato Baldelli, and Francesco Flammini

Author Index .................................................. 481