Preface

Welcome to SAFECOMP 2005, held in Fredrikstad, Norway. Since its establishment SAFECOMP, the series of conferences on Computer Safety, Reliability and Security, has contributed to the progress of the state of the art in dependable applications of computer systems. SAFECOMP provides ample opportunity to exchange insights and experiences in emerging methods and practical experience across the borders of different disciplines. Previous SAFECOMP's have year after year registered new multidisciplinary trends on dependability of computer-based systems.

SAFECOMP 2005 focused on dependability of critical computer applications and was a platform for knowledge and technology transfer between academia, industry and research institutions. Papers were invited on all aspects of dependability and survivability of critical computer-based systems in various branches and infrastructures. Due to the increasing awareness and importance of security issues of critical computer-based systems, SAFECOMP 2005 emphasized work in this area. Nowadays practical experience points out the need for multidisciplinary approaches to deal with the nature of critical complex settings.

The SAFECOMP 2005 program consisted of 30 papers selected from 84 submissions. The 30 papers represented scientists from 14 different countries acknowledging the world-wide interest of SAFECOMP and the addressed topics. The SAFECOMP program was supplemented by keynote talks enhancing the technical and scientific merit of the conference, a number of co-located activities, meetings and tutorials, and a technical visit to the research environment in Halden which organized the conference.

We would like to thank the International Program Committee, the external reviewers, the keynote speakers, and the authors for their work in support of SAFECOMP 2005. We would also like to thank the conference staff at the Institute of Energy Technology and Østfold University College. We really enjoyed the work, and we hope you appreciated the care we put into organizing the conference. Finally, we would like to extend to you the invitation to attend and contribute to SAFECOMP 2006 in Gdansk, Poland (www.safecomp.org).

July 2005

Gustav Dahll
Bjørn Axel Gran
Rune Winther
Organization

SAFECOMP 2005 Organization

General Chair
Gustav Dahll, Norway

Program Co-chairs
Bjørn Axel Gran, Norway
Rune Winther, Norway

EWICS Chair
Udo Voges, Germany

Organizing Committee
Rune Fredriksen, Norway
Siv-Hilde Houmb, Norway
Monica Kristiansen, Norway
John Petter Kvalvik, Norway
Jørn L. Pettersen, Norway
Atoosa P.-J. Thunem, Norway
Bjørn Axel Gran, Norway
Rune Winther, Norway

Institute for Energy Technology
Høgskolen i Østfold
International Program Committee

Stuart Anderson, UK
Terje Aven, Norway
Ramesh Bharadwaj, USA
Robin Bloomfield, UK
Sandro Bologna, Italy
Andrea Bondavalli, Italy
Inga-Lill Bratteby-Ribbing, Sweden
Bettina Buth, Germany
Stefan Christiernin, Sweden
Gustav Dahl, Norway
Peter Daniel, UK
Massimo Felici, UK
Robert Genser, Austria
Chris Goring, UK
Januszcz Gorski, Poland
Bjorn Axel Gran, Norway
Wolfgang Grieskamp, USA
Wolfgang Halang, Germany
Kai Hansen, Norway
Monika Heiner, Germany
Mariotta Heisel, Germany
Connie Heitmeyer, USA
Atte Helminen, Finland
Peter Jacobsson, Sweden
Ole-Arnt Johnsen, Norway
Chris Johnson, UK
Erland E. Jonsson, Sweden
Mohamed Kaâniche, France
Karama Kanoun, France
Martin Kropic, Czech Republic
Kenneth Kvønnesland, Norway
Dennis Kügler, Germany
Peter B. Ladkin, Germany
Peter Luggesmeyer, Germany
Oliver Mäckel, Germany
Meine van der Meulen, UK
Odd Nordland, Norway
Jan G. Nordstrøm, Norway
Alberto Pasquini, Italy
Gerd Rabe, Germany
Felix Redmill, UK
Judith Rossebo, Norway
Martin Rothfelder, Germany
Francesca Saglietti, Germany
Erwin Schoitsch, Austria
Terje Sivertsen, Norway
Jeanine Souquières, France
Werner Stephan, Germany
Ketil Stølen, Norway
Tor Stålhane, Norway
Asuman Suenbuel, USA
Mark Sujan, UK
Thomas Santen, Germany
Atoosa P.-J. Thunem, Norway
Jos Trienekens, The Netherlands
Adolfo Villaflorita, Italy
Udo Voges, Germany
Albrecht Weinert, Germany
Marc Wilikens, Italy
Rune Winther, Norway
Stefan Wittmann, Germany
Eric Wong, USA
Zdzislaw Zurakowski, Poland

External Reviewers

Matthias Anlauf
Terje Andersen
Lassaad Cheikhrouhou
Silvano Chiaradonna
Felicità Di Giandomenico
Lorenzo Falai
Siv-Hilde Hounb
Martin Gilje Jaatun
Terje Jensen
Tor Hjalmar Johannotensen
Mass Soldal Lund
Tom Lysemose
Andreas Nonnengart
Simone Pozzi
Yu Qi
Atle Refsdal
Georg Rock
Luca Save
Fredrik Seehusen
Nikolai Tillmann
Inger Anne Tøndel
Fredrik Vraalsen
Linzhang Wang
Sponsoring Organizations

Scientific Sponsor

Scientific Co-sponsors

The Research Council of Norway

seibersdorf research
An enterprise of the Austrian Research Centers.

NTNU
Norwegian University of Science and Technology
telenor

IFIP WG10.4 on Dependable Computing and Fault Tolerance
IFIP WG13.5 on Human Error, Safety and System Development

Halden IT Forum
SCSC - Safety-Critical Systems Club
SRMC - Software Reliability & Metrics Club
NONSTOPP - NOrsk Nettverk for Sikre Trygge Og Pålidelige Programmerbare Systemer
CMMI RAMS Extension Based on CENELEC Railway Standard
  Jose Antonio Fonseca, Jorge Rady de Almeida Júnior ............... 1

The Importance of Single-Source Engineering of Emergency
and Process Shutdown Systems
  Robert Martinez, Torgeir Enkerud................................. 13

Combining Extended UML Models and Formal Methods to Analyze
Real-Time Systems
  Nawal Addouche, Christian Antoine, Jacky Montmain............. 24

Defining and Decomposing Safety Policy for Systems of Systems
  Martin Hall-May, Tim P. Kelly .................................. 37

Generalising Event Trees Using Bayesian Networks with a Case Study
of Train Derailment
  George Bearfield, William Marsh ................................. 52

Control and Data Flow Testing on Function Block Diagrams
  Eunkyoung Jee, Junbeom Yoo, Sungdeok Cha ...................... 67

Comparing Software Measures with Fault Counts Derived from
Unit-Testing of Safety-Critical Software
  Wolfgang Herzner, Stephan Ramberger, Thomas Länger,
  Christian Reumann, Thomas Gruber, Christian Sejkora........... 81

Automatic Analysis of a Safety Critical Tele Control System
  Edoardo Campagnano, Ester Ciancamerla, Michele Minichino,
  Enrico Tronci ................................................. 94

A Formal Model for Fault-Tolerance in Distributed Systems
  Brahim Hamid, Mohamed Mosbah ................................. 108

Model-Based Safety Analysis of Simulink Models Using SCADE Design
Verifier
  Anjali Joshi, Mats P.E. Heimdahl................................. 122

Using Safety Critical Artificial Neural Networks in Gas Turbine
Aero-Engine Control
  Zeshan Kurd, Tim P. Kelly ...................................... 136
On the Effectiveness of Run-Time Checks
  Meine J.P. van der Meulen, Lorenzo Strigini, Miguel A. Revilla .... 151

A Technique for Fault Tolerance Assessment of COTS Based Systems
  Ruben Alexandersson, D. Krishna Chaitanya, Peter Öhman,
  Yasir Siraj .......................................................... 165

Finding Upper Bounds for Software Failure Probabilities – Experiments
  and Results
  Monica Kristiansen .......................................... 179

Justification of Smart Sensors for Nuclear Applications
  Peter Bishop, Robin Bloomfield, Sofia Guerra, Kostas Tourlas .... 194

Evolutionary Safety Analysis: Motivations from the Air Traffic
  Management Domain
  Massimo Felici ................................................ 208

Public-Key Cryptography and Availability
  Tage Stabell-Kulø, Simone Lupetti ........................... 222

End-To-End Worst-Case Response Time Analysis for Hard Real-Time
  Distributed Systems
  Lei Wang, Mingde Zhao, Zengwei Zheng, Zhaohui Wu ............. 233

Safety Interfaces for Component-Based Systems
  Jonas Elmqvist, Simin Nadjm-Tehrani, Marius Minea ............ 246

A Safety-Related PES for Task-Oriented Real-Time Execution Without
  Asynchronous Interrupts
  Martin Skambraks ............................................. 261

Are High-Level Languages Suitable for Robust Telecoms Software?
  J.H. Nyström, P.W. Trinder, D.J. King ......................... 275

Functional Apportioning of Safety Requirements on Railway Signalling
  Systems
  Ola Løkberg, Øystein Skogstad ................................ 289

Automatic Code Generation for PLC Controllers
  Krzysztof Sacha .................................................. 303
The TACO Approach for Traceability and Communication of Requirements
   Terje Sivertsen, Rune Fredriksen, Atoosa P-J Thunem,
   Jan-Erik Holmberg, Janne Valkonen, Olli Ventä,
   Jan-Ove Andersson ................................................. 317

An IEC 62061 Compliant Safety System Design Method for Machinery
   Bengt Ljungquist, Thomas Thelin .................................. 330

   Tom Gilb ................................................................. 344

The Application of an Object-Oriented Method in Information System Security Evaluation
   Qiang Yan, Hua-ying Shu ............................................. 357

Towards a Cyber Security Reporting System – A Quality Improvement Process
   Jose J. Gonzalez .......................................................... 368

Security Research from a Multi-disciplinary and Multi-sectoral Perspective
   Atoosa P-J Thunem ..................................................... 381

Problem Frames and Architectures for Security Problems
   Denis Hatebur, Maritta Heisel ....................................... 390

Author Index ............................................................... 405