Since 1979, when it was first established by the Technical Committee on Reliability, Safety and Security of the European Workshop on Industrial Computer Systems (EWICS TC7), the SAFECOMP Conference series has regularly and continuously contributed to improving the state of the art of highly dependable computer-based systems, since then increasingly applied to safety-relevant industrial domains.

In this expanding technical field SAFECOMP offers a platform for knowledge and technology transfer between academia, industry, research and licensing institutions, providing ample opportunities for exchanging insights, experiences and trends in the areas of safety, reliability and security regarding critical computer applications. In accordance with the growing spread of critical infrastructures involving both safety and security threats, this year’s SAFECOMP program included a considerable number of contributions addressing technical problems and engineering solutions across the border between safety-related and security-related concerns.

The reaction to our call for papers was particularly gratifying and impressive, including 136 full papers submitted by authors representing 29 countries from Europe, Asia, North and South America as well as Australia. The selection of 33 full papers and 16 short papers for presentation and publication was a challenging task requiring a huge amount of reviewing and organizational effort. In view of the particularly high number of articles submitted, obvious practical constraints led – to our regret – to the rejection of a considerable amount of high-quality work. To all authors, invited speakers, members of the International Program Committee and external reviewers go our heartfelt thanks!

The local organization of SAFECOMP 2007, hosted in Nuremberg, is also gratefully acknowledged. The intensive preparatory activities demanded year-long dedication from the members of the Department of Software Engineering at the University of Erlangen-Nuremberg, which co-organized the event in co-operation with the German Computer Society (Gesellschaft für Informatik). Particular thanks are due to all colleagues and friends from the Organizing Committee, whose support we regard as crucial for the success of this conference.

We are confident that – when reading the present volume of the Lecture Notes in Computer Science – you will find its contents interesting enough to consider joining the SAFECOMP community. In the name of EWICS TC7 and of the future organizers we welcome you and invite you to attend future SAFECOMP conferences – among them SAFECOMP 2008 in Newcastle upon Tyne (UK) – and to contribute actively to their technical program.

July 2007

Francesca Saglietti
Norbert Oster
Organization

Program Chair
Francesca Saglietti (Germany)

EWICS Chair
Udo Voges (Germany)

International Program Committee

Stuart Anderson (UK)  Floor Koornneef (The Netherlands)
Robin Bloomfield (UK)  Peter B. Ladkin (Germany)
Sandro Bologna (Italy)  Søren Lindskov Hansen (Denmark)
Jens Braband (Germany)  Bev Littlewood (UK)
Inga Bratteby-Ribbing (SE)  Vic Maggioli (USA)
Bettina Buth (Germany)  Odd Nordland (Norway)
Peter Daniel (UK)  Gerd Rabe (Germany)
Christian Diedrich (Germany)  Felix Redmill (UK)
Jana Dittmann (Germany)  Martin Rothfelder (Germany)
Wolfgang Ehrenberger (Germany)  Krzysztof Sacha (Poland)
Massimo Felici (UK)  Erwin Schoitsch (Austria)
Robert Genser (Austria)  Werner Stephan (Germany)
Bjorn Axel Gran (Norway)  Mark Sujan (UK)
Karl-Erwin Großpietsch (Germany)  Pascal Traverse (France)
Wolfgang Halang (Germany)  Jos Trienekens (The Netherlands)
Monika Heiner (Germany)  Meine Van der Meulen
Maritza Heisel (Germany)  (The Netherlands)
Constance Heitmeyer (USA)  Udo Voges (Germany)
Janusz Gorski (Poland)  Albrecht Weinert (Germany)
Karl-Heinz John (Germany)  Rune Winther (Norway)
Karama Kanoun (France)  Stefan Wittmann (Belgium)
Zdzislaw Zurakowski (Poland)

Organizing Committee
Francesca Saglietti (Co-chair)
Wolfgang Ehrenberger (Co-chair)
Norbert Oster
Jutta Radke
Gerd Schober
Sven Söhnlein
## External Reviewers

<table>
<thead>
<tr>
<th>Myla Archer</th>
<th>Andreas Nonnengart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lassaad Cheikhrouhou</td>
<td>Andrea Oermann</td>
</tr>
<tr>
<td>DeJiu Chen</td>
<td>Ulf Olsson</td>
</tr>
<tr>
<td>Yves Crouzet</td>
<td>Norbert Oster</td>
</tr>
<tr>
<td>Håkan Edler</td>
<td>Christian Raspotnig</td>
</tr>
<tr>
<td>Jonas Elmqvist</td>
<td>Ronny Richter</td>
</tr>
<tr>
<td>Denis Hatebur</td>
<td>Georg Rock</td>
</tr>
<tr>
<td>Tobias Hoppe</td>
<td>Jan Sanders</td>
</tr>
<tr>
<td>Ralph D. Jeffords</td>
<td>Thomas Santen</td>
</tr>
<tr>
<td>Björn Johansson</td>
<td>Tobias Scheidat</td>
</tr>
<tr>
<td>Johan Karlsson</td>
<td>Holger Schmidt</td>
</tr>
<tr>
<td>Stefan Kiltz</td>
<td>Bernd Schomburg</td>
</tr>
<tr>
<td>Andreas Lang</td>
<td>Martin Schwarick</td>
</tr>
<tr>
<td>Bruno Langenstein</td>
<td>Dirk Seifert</td>
</tr>
<tr>
<td>Tiejun Ma</td>
<td>Sven Söhnlein</td>
</tr>
<tr>
<td>Oliver Meyer</td>
<td>Marc Spisländer</td>
</tr>
<tr>
<td>M. Oliver Möller</td>
<td>Mirco Tribastone</td>
</tr>
<tr>
<td>Simin Nadjm-Tehrani</td>
<td>Arno Wacker</td>
</tr>
<tr>
<td>Vincent Nicomette</td>
<td>Dirk Wischermann</td>
</tr>
</tbody>
</table>
**Scientific Sponsor**

EWICS – European Workshop on Industrial Computer Systems  
TC7 – Technical Committee on Reliability, Safety and Security

in collaboration with the following **Scientific Co-sponsors**:

**IFAC**  
International Federation of Automatic Control

**IFIP**  
International Federation for Information Processing

**ENCRESS**  
European Network of Clubs for Reliability and Safety of Software-Intensive Systems

**SCSC**  
The Safety-Critical Systems Club

**SRMC**  
The Software Reliability & Metrics Club

**OCG**  
Austrian Computer Society

**DECOS**  
Dependable Embedded Components and Systems
SAFECOMP 2007 Organizers

SWE
Department of Software Engineering
University of Erlangen-Nuremberg

GI
Gesellschaft für Informatik e.V.
Table of Contents

Safety Cases

Establishing Evidence for Safety Cases in Automotive Systems – A Case Study .......................... 1
Willem Ridderhof, Hans-Gerhard Gross, and Heiko Doerr

Goal-Based Safety Cases for Medical Devices: Opportunities and Challenges .......................... 14
Mark-Alexander Sujan, Floor Koornneef, and Udo Voges

Impact of Security on Safety

Richard Robinson, Mingyan Li, Scott Lintelman, Krishna Sampigethaya, Radha Poovendran, David von Oheimb, Jens-Uwe Bußer, and Jorge Cuellar

Andreas Lang, Jana Dittmann, Stefan Kiltz, and Tobias Hoppe

Modelling Interdependencies Between the Electricity and Information Infrastructures ...................... 54
Jean-Claude Laprie, Karama Kanoun, and Mohamed Kaâniche

Poster Session 1

Handling Malicious Code on Control Systems ........................................... 68
Wan-Hui Tseng and Chin-Feng Fan

Management of Groups and Group Keys in Multi-level Security Environments ......................... 75
Mohammad Alhammouri and Sead Muftic

Application of the XTT Rule-Based Model for Formal Design and Verification of Internet Security Systems .................. 81
Grzegorz J. Nalepa

RAMSS Analysis for a Co-operative Integrated Traffic Management System ............................... 87
Armin Selhofer, Thomas Gruber, Michael Putz, Erwin Schoitsch, and Gerald Sonneck
# Table of Contents

Combining Static/Dynamic Fault Trees and Event Trees Using Bayesian Networks ................................. 93
  *S.M. Hadi Hosseini and Makoto Takahashi*

Component Fault Tree Analysis Resolves Complexity: Dependability Confirmation for a Railway Brake System .................................................. 100
  *Reiner Heilmann, Stefan Rothbauer, and Ariane Sutor*

**Fault Tree Analysis**

Compositional Temporal Fault Tree Analysis .................................................. 106
  *Martin Walker, Leonardo Bottaci, and Yiannis Papadopoulos*

Representing Parameterised Fault Trees Using Bayesian Networks ............ 120
  *William Marsh and George Bearfield*

Human Error Analysis Based on a Semantically Defined Cognitive Pilot Model .................................................. 134
  *Andreas Lüdtke and Lothar Pfeifer*

**Safety Analysis**

Safety Analysis of Safety-Critical Software for Nuclear Digital Protection System .................................................. 148
  *Gee-Yong Park, Jang-Soo Lee, Se-Woo Cheon, Kee-Choon Kwon, Eunkyoung Jee, and Kwang Yong Koh*

Specification of a Software Common Cause Analysis Method ................. 162
  *Rainer Faller*

Combining Bayesian Belief Networks and the Goal Structuring Notation to Support Architectural Reasoning About Safety .................. 172
  *Weihang Wu and Tim Kelly*

Application of Interactive Cause and Effect Diagrams to Safety-Related PES in Industrial Automation .................................................. 187
  *Hans Russo and Andreas Turk*

**Security Aspects**

Survival by Deception .................................................. 197
  *Martin Gilje Jaatun, Åsmund Ahlmann Nyre, and Jan Tore Sørensen*

How to Secure Bluetooth-Based Pico Networks .................................................. 209
  *Dennis K. Nilsson, Phillip A. Porras, and Erland Jonsson*
Learning from Your Elders: A Shortcut to Information Security Management Success ................................................................. 224  
*Finn Olav Sveen, Jose Manuel Torres, and Jose Maria Sarriegi*

Intrusion Attack Tactics for the Model Checking of e-Commerce Security Guarantees ................................................................. 238  
*Stylianos Basagiannis, Panagiotis Katsaros, and Andrew Pombortsis*

**Poster Session 2**

Safety Process Improvement with POSE and Alloy .......................... 252  
*Derek Mannering, Jon G. Hall, and Lucia Rapanotti*

Defense-in-Depth and Diverse Qualification of Safety-Critical Software ................................................................. 258  
*Horst Miedl, Jang-Soo Lee, Arndt Lindner, Ernst Hoffman, Josef Martz, Young-Jun Lee, Jong-Gyun Choi, Jang-Yeol Kim, Kyoung-Ho Cha, Se-Woo Cheon, Cheol-Kwon Lee, Gee-Yong Park, and Kee-Choon Kwon*

Experimental Evaluation of the DECOS Fault-Tolerant Communication Layer ................................................................. 264  
*Jonny Vinter, Henrik Eriksson, Astrit Ademaj, Bernhard Leiner, and Martin Schlager*

Achieving Highly Reliable Embedded Software: An Empirical Evaluation of Different Approaches ................................................................. 270  
Falk Salewski and Stefan Kowalewski

Modeling, Analysis and Testing of Safety Issues - An Event-Based Approach and Case Study ................................................................. 276  
Fevzi Belli, Axel Hollmann, and Nimal Nissanke

A Concept for a Safe Realization of a State Machine in Embedded Automotive Applications ................................................................. 283  
Jürgen Mottok, Frank Schiller, Thomas Völkl, and Thomas Zeitler

**Verification and Validation**

Safety Demonstration and Software Development .......................... 289  
Jean-Claude Laprie

Improving Test Coverage for UML State Machines Using Transition Instrumentation ................................................................. 301  
Mario Friske and Bernd-Holger Schlingloff

Verification of Distributed Applications ................................................................. 315  
Bruno Langenstein, Andreas Nonnengart, Georg Rock, and Werner Stephan
Platform Reliability

Analysis of Combinations of CRC in Industrial Communication .............. 329
   Tina Mattes, Jörg Pfahler, Frank Schiller, and Thomas Honold

A Comparison of Partitioning Operating Systems for Integrated Systems ........................................................ 342
   Bernhard Leiner, Martin Schlager, Roman Obermaisser, and Bernhard Huber

Software Encoded Processing: Building Dependable Systems with Commodity Hardware ......................... 356
   Ute Wappler and Christof Fetzer

Reliability Evaluation

Reliability Modeling for the Advanced Electric Power Grid .................. 370
   Ayman Z. Faza, Sahra Sedigh, and Bruce M. McMillin

Case Study on Bayesian Reliability Estimation of Software Design of Motor Protection Relay ..................... 384
   Atte Helminen

A Reliability Evaluation of a Group Membership Protocol .............. 397
   Valério Rosset, Pedro F. Souto, Paulo Portugal, and Francisco Vasques

Poster Session 3

Bounds on the Reliability of Fault-Tolerant Software Built by Forcing Diversity ................................................. 411
   Kizito Salako

A Tool for Network Reliability Analysis ........................................ 417
   Andrea Bobbio, Roberta Terruggia, Andrea Boellis, Ester Ciancamerla, and Michele Minichino

DFT and DRBD in Computing Systems Dependability Analysis .......... 423
   Salvatore Distefano and Antonio Puliafito

Development of Model Based Tools to Support the Design of Railway Control Applications .......................... 430
   István Majzik, Zoltán Micskei, and Gergely Pintér

Formal Methods

Formal Specification and Analysis of AFDX Redundancy Management Algorithms ........................................... 436
   Jan Täubrich and Reinhard von Hanxleden
Modeling and Automatic Failure Analysis of Safety-Critical Systems
Using Extended Safecharts .................................................. 451
  Yean-Ru Chen, Pao-Ann Hsiung, and Sao-Jie Chen

Using Deductive Cause-Consequence Analysis (DCCA) with SCADE ... 465
  Matthias Güdemann, Frank Ortmeier, and Wolfgang Reif

**Static Code Analysis**

Experimental Assessment of Astrée on Safety-Critical Avionics
Software ................................................................. 479
  Jean Souyris and David Delmas

Detection of Runtime Errors in MISRA C Programs: A Deductive
Approach ................................................................. 491
  Ajith K. John, Babita Sharma, A.K. Bhattacharjee,
  S.D. Dhodapkar, and S. Ramesh

**Safety-Related Architectures**

A Taxonomy for Modelling Safety Related Architectures in Compliance
with Functional Safety Requirements ................................. 505
  Jesper Berthing and Thomas Maier

Controller Architecture for Safe Cognitive Technical Systems ....... 518
  Sebastian Kain, Hao Ding, Frank Schiller, and Olaf Stursberg

Improved Availability and Reliability Using Re-configuration Algorithm
for Task or Process in a Flight Critical Software .................... 532
  Ananda Challaghatta Muniyappa

**Author Index** ......................................................... 547