

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Michael D. Harrison Mark-Alexander Sujan (Eds.)

# Computer Safety, Reliability, and Security

27th International Conference, SAFECOMP 2008  
Newcastle upon Tyne, UK, September 22-25, 2008  
Proceedings

## Volume Editors

Michael D. Harrison  
Newcastle University  
School of Computing Science  
Claremont Tower, Newcastle upon Tyne, NE1 7RU, UK  
E-mail: michael.harrison@ncl.ac.uk

Mark-Alexander Sujan  
University of Warwick  
Health Sciences Research Institute  
Coventry, CV4 7AL, UK  
E-mail: m-a.sujan@warwick.ac.uk

Library of Congress Control Number: 2008934760

CR Subject Classification (1998): D.1-4, E.4, C.3, F.3, K.6.5

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743  
ISBN-10 3-540-87697-9 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-87697-7 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media  
springer.com

© Springer-Verlag Berlin Heidelberg 2008  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12517558 06/3180 5 4 3 2 1 0

# Preface

Safecomp was held in Newcastle upon Tyne, UK in September 2008. The conference was the latest in a long and strong tradition of leading-edge research and practice in Computer Safety, Reliability and Security that began in 1979.

The programme was drawn from a strong international selection of papers from a dozen countries in three continents (32 papers from 115 submissions). Traditional Safecomp themes such as software dependability, software safety arguments and formal methods continued to be represented. This conference also strengthened themes that have been less visible in previous Safecomp conferences, particularly those relating to the complexity and resilience of systems, critical infrastructures and human factors. It broadened the usual domains of application to include, for example, e-Commerce. The programme continued to benefit from strong industrial contributions in safety critical and security critical applications.

We were fortunate to have keynote addresses from Colin O'Halloran (QinetiQ) and Roger Rivett (LandRover) on different complementary industrial experiences in security and reliability. We were also fortunate to have Erik Hollnagel as our opening keynote speaker. Professor Hollnagel's contribution was effective in challenging traditional views, broadening the focus of concern, especially relating to the management and analysis of complexity in large-scale systems.

We would like to express our gratitude and thanks to all those whose effort has made this conference possible: to the submitting authors and to the invited speakers; to the Programme Committee and the external reviewers who helped compile an attractive programme; to the financial and scientific sponsors; and last but not least, to the members of the Organizing Committee who took care of the local arrangements.

We hope that you will find these proceedings of interest and use for your own work.

July 2008

Michael Harrison  
Mark-Alexander Sujjan

# Organization

Safecomp 2008 was sponsored by EWICS TC7.

## Organizing Committee

Co-chairs	Michael Harrison (Newcastle University, UK) Mark-Alexander Sujan (Warwick University, UK)
EWICS Chair	U. Voges (Forschungszentrum Karlsruhe, DE)
Organizing Committee	Joan Atkinson (Newcastle University, UK) Massimo Felici (University of Edinburgh, UK) Michael Harrison (Newcastle University, UK) Steve Riddle (Newcastle University, UK) Claire Smith (Newcastle University, UK) Shamus Smith (Durham University, UK) Mark-Alexander Sujan (Warwick University, UK) Christine Wisher (Newcastle University, UK) Nikos Zarboutis (ENERCON Service Hellas, Greece)

## Programme Committee

R. Amalberti, France	M. Heisel, Germany	S. Pozzi, Italy
S. Anderson, UK	C. Heitmeyer, USA	G. Rabe, Germany
T. Anderson, UK	A. Hessami, UK	F. Redmill, UK
J. Braband, Germany	E. Hollnagel, France	F. Saglietti, Germany
N. Buth, Germany	C. Johnson, UK	E. Schoitsch, Austria
S. Cheshire, UK	M. Kaaniche, France	S. Smith, UK
M. Cooke, UK	K. Kanoun, France	L. Strigini, UK
P. Daniel, UK	T. Kelly, UK	M. Sujan, UK
W. Ehrenberger, Germany	J. Knight, USA	P. Traverse, France
L. Emmet, UK	F. Koornneef, The Netherlands	J. Trienekens, The Netherlands
C. Fairburn, UK	P. Ladkin, Germany	M. van der Meulen, The Netherlands
M. Felici, UK	B. Littlewood, UK	U. Voges, Germany
J. Gorski, Poland	J. McDermid, UK	A. Weinert, Germany
B. Gran, Norway	O. Nordland, Norway	S. Wittmann, Belgium
L. Grunske, Germany	P. Palanque, France	N. Zarboutis, Greece
W. Halang, Germany	A. Pasquini, Italy	Z. Zurakowski, Poland
M. Harrison, UK	M. Pickering, UK	

## External Reviewers

O. Meyer	I. Wentzlauff	N. Rivire
N. Chozos	T. Santen	M. Roy
T. Storer	H. Schmidt	A. van Moorsel
T. Ma	D. Hatebur	C. Gacek
J. Clark	T. Santen	P. Ryan

## Sponsoring Institutions

EWICS TC7	
Centre for Software Reliability	
Newcastle University	
Warwick Medical School	
AdaCore	
ReSIST	
Qinetiq	
Adelard	
TTE-Systems	
British Computer Society	
ifip	
IFAC	
DECOS	

Austrian Computer society



Gesellschaft für Informatik e.V.



Enress



# Table of Contents

## Keynote Papers

Critical Information Infrastructures: Should Models Represent Structures or Functions? .....	1
<i>Erik Hollnagel</i>	
Security and Interoperability for MANETs and a Fixed Core .....	5
<i>Colin O'Halloran and Andy Bates</i>	
Technology, Society and Risk .....	12
<i>Roger Rivett</i>	
Panel: Complexity and Resilience .....	13
<i>Aad van Moorsel</i>	

## Software Dependability

The Effectiveness of T-Way Test Data Generation .....	16
<i>Michael Ellims, Darrel Ince, and Marian Petre</i>	
Towards Agile Engineering of High-Integrity Systems .....	30
<i>Richard F. Paige, Ramon Charalambous, Xiaocheng Ge, and Phillip J. Brooke</i>	
SafeSpection – A Systematic Customization Approach for Software Hazard Identification .....	44
<i>Christian Denger, Mario Trapp, and Peter Liggesmeyer</i>	
Integrating Safety Analyses and Component-Based Design .....	58
<i>Dominik Domis and Mario Trapp</i>	
Modelling Support for Design of Safety-Critical Automotive Embedded Systems .....	72
<i>DeJiu Chen, Rolf Johansson, Henrik Lönn, Yiannis Papadopoulos, Anders Sandberg, Fredrik Törner, and Martin Törngren</i>	

## Resilience

Resilience in the Aviation System .....	86
<i>Antonio Chialastri and Simone Pozzi</i>	
Resilience Markers for Safer Systems and Organisations .....	99
<i>Jonathan Back, Dominic Furniss, Michael Hildebrandt, and Ann Blandford</i>	



Modeling and Analyzing Disaster Recovery Plans as Business Processes ..... 113  
*Andrzej Zalewski, Piotr Sztandera, Marcin Ludzia, and Marek Zalewski*

**Fault Tolerance**

Analysis of Nested CRC with Additional Net Data in Communication ..... 126  
*Tina Mattes, Frank Schiller, Annemarie Mörwald, and Thomas Honold*

Symbolic Reliability Analysis of Self-healing Networked Embedded Systems ..... 139  
*Michael Glaß, Martin Lukasiewicz, Felix Reimann, Christian Haubelt, and Jürgen Teich*

Investigation and Reduction of Fault Sensitivity in the FlexRay Communication Controller Registers ..... 153  
*Yasser Sedaghat and Seyed Ghassem Miremadi*

**Security**

Secure Interaction Models for the HealthAgents System ..... 167  
*Liang Xiao, Paul Lewis, and Srinandan Dasmahapatra*

Security Challenges in Adaptive e-Health Processes ..... 181  
*Michael Predeschly, Peter Dadam, and Hilmar Acker*

An Efficient e-Commerce Fair Exchange Protocol That Encourages Customer and Merchant to Be Honest ..... 193  
*Abdullah Alaraj and Malcolm Munro*

Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles ..... 207  
*Dennis K. Nilsson, Ulf E. Larson, and Erland Jonsson*

Finding Corrupted Computers Using Imperfect Intrusion Prevention System Event Data ..... 221  
*Danielle Chrun, Michel Cukier, and Gerry Sneeringer*

Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures ..... 235  
*Tobias Hoppe, Stefan Kiltz, and Jana Dittmann*

**Safety Cases**

Constructing a Safety Case for Automatically Generated Code from Formal Program Verification Information ..... 249  
*Nurlida Basir, Ewen Denney, and Bernd Fischer*

Applying Safety Goals to a New Intensive Care Workstation System . . . . .	263
<i>Uwe Becker</i>	
Safety Assurance Strategies for Autonomous Vehicles . . . . .	277
<i>Andrzej Wardziński</i>	
Expert Assessment of Arguments: A Method and Its Experimental Evaluation . . . . .	291
<i>Lukasz Cyra and Janusz Górski</i>	

## Formal Methods

Formal Verification by Reverse Synthesis . . . . .	305
<i>Xiang Yin, John C. Knight, Elisabeth A. Nguyen, and Westley Weimer</i>	
Deriving Safety Software Requirements from an AltaRica System Model . . . . .	320
<i>Sophie Humbert, Christel Seguin, Charles Castel, and Jean-Marc Bosc</i>	
Model-Based Implementation of Real-Time Systems . . . . .	332
<i>Krzysztof Sacha</i>	
Early Prototyping of Wireless Sensor Network Algorithms in PVS . . . . .	346
<i>Cinzia Bernardeschi, Paolo Masci, and Holger Pfeifer</i>	

## Dependability Modelling

Analyzing Fault Susceptibility of ABS Microcontroller . . . . .	360
<i>Dawid Trawczynski, Janusz Sosnowski, and Piotr Gawkowski</i>	
A Formal Approach for User Interaction Reconfiguration of Safety Critical Interactive Systems . . . . .	373
<i>David Navarre, Philippe Palanque, and Sandra Basnyat</i>	
The Wrong Question to the Right People. A Critical View of Severity Classification Methods in ATM Experimental Projects . . . . .	387
<i>Alberto Pasquini, Simone Pozzi, and Luca Sava</i>	

## Security and Dependability

A Context-Aware Mandatory Access Control Model for Multilevel Security Environments . . . . .	401
<i>Jafar Haadi Jafarian, Morteza Amini, and Rasool Jalili</i>	

Formal Security Analysis of Electronic Software Distribution Systems . . .	415
<i>Monika Maidl, David von Oheimb, Peter Hartmann, and Richard Robinson</i>	
The Advanced Electric Power Grid: Complexity Reduction Techniques for Reliability Modeling . . . . .	429
<i>Ayman Z. Faza, Sahra Sedigh, and Bruce M. McMillin</i>	
Automating the Processes of Selecting an Appropriate Scheduling Algorithm and Configuring the Scheduler Implementation for Time-Triggered Embedded Systems . . . . .	440
<i>Ayman K. Gendy and Michael J. Pont</i>	
<b>Author Index . . . . .</b>	<b>455</b>