Lecture Notes in Computer Science 5219

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

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

Springer

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

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 Sujan

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

External Reviewers

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

Encress

Table of Contents

Keynote Papers

Software Dependability

Resilience

Fault Tolerance

Security

Safety Cases

Formal Methods

Dependability Modelling

Security and Dependability