

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

Microsoft Research, Cambridge, 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

Bettina Buth Gerd Rabe Till Seyfarth (Eds.)

Computer Safety, Reliability, and Security

28th International Conference, SAFECOMP 2009
Hamburg, Germany, September 15-18, 2009
Proceedings

Volume Editors

Bettina Buth

Department of Informatik, Faculty TI

HAW Hamburg

Hamburg, Germany

E-mail: buth@informatik.haw-hamburg.de

Gerd Rabe

TÜV Nord SysTec GmbH & Co. KG

Competence Center Digital I&C Systems

SEELAB Software and Electronics Laboratory

Hamburg, Germany

E-mail: grabe@tuev-nord.de

Till Seyfarth

TÜV Nord SysTec GmbH & Co. KG

Competence Center Digital I&C Systems

SEELAB Software and Electronics Laboratory

Hamburg, Germany

E-mail: tseyfarth@tuev-nord.de

Library of Congress Control Number: 2009934307

CR Subject Classification (1998): B.8, C.4, D.2.4, D.4.5, H.2.7, K.4.4, K.6.5, D.4.6

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743

ISBN-10 3-642-04467-0 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-04467-0 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.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12753260 06/3180 5 4 3 2 1 0

Preface

Computer-based systems have become omnipresent commodities within our environment. While for a large variety of these systems such as transportation systems, nuclear or chemical plants, or medical systems their relation to safety is obvious, we often do not reflect that others are as directly related to risks concerning harm done to persons or matter as, for example, elevator control or mobile phones. At least we are not aware of the risk in our daily use of them.

Safecomp as a community and a conference series has accompanied this development for 30 years up to Safecomp 2009, which was the 28th of the series. During this time the topics and methods as well as the community have undergone changes. These changes reflect the requirements of the above-mentioned ubiquitous presence of safety-related systems. Safecomp has always encouraged and will further encourage academia and industry to share and exchange their ideas and experiences.

After 30 years, we as the organizers of Safecomp 2009, found it imperative to take stock: which methods found their way into the application areas; which new approaches need to be checked for their practical applicability. As different application domains developed their own approaches over the previous decades, we tried to attract people with different backgrounds for this conference. Although the years 2008 and 2009 were not easy with regard to the overall global economic situation, we succeeded with this goal.

We received 72 contributions from 14 countries, including 33 contributions from industry and research agencies. Of these, we selected 25 for the presentation as conference talks and for these proceedings. We invited two persons with a practical and theoretical background to provide the invited talks—our special thanks to Anne Haxthausen and Walt Boyes for their time and effort. The International Programme Committee further decided to include a joint session with the GfSE (Gesellschaft für Systems Engineering, German chapter of INCOSE) on model-based systems engineering in the conference programme in order to emphasize the system aspect and initiate a new liason. Unfortunately, it was not possible to include the related material in these proceedings since the session had a workshop character. Taking all this into account, we are positive that readers of these proceedings will gain as much insight into the current state of the art in safety engineering within various relevant application domains as the participants of the conference already have.

We would like to thank the International Programme Committee and the external reviewers for their work and the constructive comments regarding both the conference organization and the improvement of individual papers for Safecomp 2009. We look forward to further joint work for future Safecomp conferences. Special thanks go to Massimo Felici, who maintained the Cyberchair interface for the conference organization and always reacted immediately to any of our

questions or cries for help. We would also like to thank those people at HAW Hamburg without whom the conference website would not have worked at all, especially Norbert Kasperczyk-Borgmann and Oliver Neumann. Last but not least we would like to thank Clarissa Hörnke and Markus Schweers of the TÜV NORD Akademie for supporting the local organization, registration and financial aspects of the conference.

During the organization of the conference and the preparation of these proceedings there were times where we were in panic and times where we had a lot of fun. Overall the fun prevailed. We do hope that this will also be the case for the local organizers of Safecom 2010 in Vienna.

July 2009

Bettina Buth
Gerd Rabe
Till Seyfarth

Organization

Programme Chair

Bettina Buth, Germany
Gerd Rabe, Germany
Till Seyfarth, Germany

Local Organization

Bettina Buth, Germany
Gerd Rabe, Germany
Till Seyfarth, Germany

EWICS Chair

Francesca Saglietti, Germany

International Programme Committee

S. Anderson, UK	T. Kelly, UK
T. Anderson, UK	J. C. Knight, USA
R. Bloomfield, UK	F. Koornneef, The Netherlands
J. Braband, Germany	P. Ladkin, Germany
B. Buth, Germany	T. Lehmann, Germany
P. Daniel, UK	S. Lindskov Hansen, Denmark
W. Ehrenberger, Germany	B. Littlewood, UK
M. Felici, UK	J. McDermid, UK
F. Flammini, Italy	O. Nordland, Norway
G. Glöe, Germany	A. Pasquini, Italy
J. Gorski, Poland	P. Pareigis, Germany
B. A. Gran, Norway	J. Peleska, Germany
W. Halang, Germany	G. Rabe, Germany
M. Harrison, UK	F. Redmill, UK
M. Heisel, Germany	F. Saglietti, Germany
C. Heitmeyer, USA	E. Schoitsch, Austria
E. Hollnagel, France	S. Schulze, Germany
M. Hübner, Germany	T. Seyfarth, Germany
C. Johnson, UK	L. Strigini, UK
M. Kaniche, France	M. Suján, UK
K. Kanoun, France	P. Traverse, France

J. Trienekens, The Netherlands

M. van der Meulen, The Netherlands

U. Voges, Germany

A. Weinert, Germany

S. Wittmann, Belgium

Z. Zurakowski, Poland

External Reviewers

O. Meyer

A. Tedeschi

R. Lock

H. Unger

A. Povyakalo

P. Hopkins

Scientific Sponsors

Austrian Research Centers

ENCRESS (European Network of Clubs for Reliability and Safety in
Software-Intensive Systems)

DECOS (Dependable Embedded Components and Systems)

GfSE (Gesellschaft für Systems Engineering)

GI (Gesellschaft für Informatik)

ifip (International Federation for Information Processing)

IFAC (International Federation for Automatic Control)

OCG (Österreichische Computer Gesellschaft)

SCSC (Safety Critical Systems Club)

Table of Contents

Invited Talks

A Domain-Specific Framework for Automated Construction and Verification of Railway Control Systems (Extended Abstract)	1
<i>Anne E. Haxthausen</i>	

Medical Systems

Model-Based Development of Medical Devices	4
<i>Uwe Becker</i>	
Why Are People's Decisions Sometimes Worse with Computer Support?	18
<i>Eugenio Alberdi, Lorenzo Strigini, Andrey A. Povyakalo, and Peter Ayton</i>	

Industrial Experience

Safety-Related Application Conditions – A Balance between Safety Relevance and Handicaps for Applications	32
<i>Friedemann Bitsch, Ulrich Feucht, and Huw Gough</i>	
Probability of Failure on Demand – The Why and the How	46
<i>Jens Braband, Rüdiger vom Hövel, and Hendrik Schübe</i>	
Establishing the Correlation between Complexity and a Reliability Metric for Software Digital I&C-Systems	55
<i>John Eidar Simensen, Christian Gerst, Bjørn Axel Gran, Josef Märtz, and Horst Miedl</i>	

Security Risk Analysis

Exploring Network Security in PROFIsafe	67
<i>Johan Åkerberg and Mats Björkman</i>	
Modelling Critical Infrastructures in Presence of Lack of Data with Simulated Annealing – Like Algorithms	81
<i>Vincenzo Fioriti, Silvia Ruzzante, Elisa Castorini, A. Di Pietro, and Alberto Tofani</i>	
Environment Characterization and System Modeling Approach for the Quantitative Evaluation of Security	89
<i>Geraldine Vache</i>	

Safety Guidelines

Experiences with the Certification of a Generic Functional Safety Management Structure According to IEC 61508.....	103
<i>Carlos G. Bilich and Zaijun Hu</i>	
Analysing Dependability Case Arguments Using Quality Models	118
<i>Michaela Huhn and Axel Zechner</i>	
Experience with Establishment of Reusable and Certifiable Safety Lifecycle Model within ABB.....	132
<i>Zaijun Hu and Carlos G. Bilich</i>	

Automotive

Automotive IT-Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats	145
<i>Tobias Hoppe, Stefan Kiltz, and Jana Dittmann</i>	
Safety Requirements for a Cooperative Traffic Management System: The Human Interface Perspective	159
<i>Thomas Gruber, Egbert Althammer, and Erwin Schoitsch</i>	

Aerospace

The COMPASS Approach: Correctness, Modelling and Performability of Aerospace Systems.....	173
<i>Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, and Marco Roveri</i>	
Formal Verification of a Microkernel Used in Dependable Software Systems	187
<i>Christoph Baumann, Bernhard Beckert, Holger Blasum, and Thorsten Bormer</i>	
Issues in Tool Qualification for Safety-Critical Hardware: What Formal Approaches Can and Cannot Do	201
<i>Brian Butka, Janusz Zalewski, and Andrew J. Kornecki</i>	

Verification, Validation, Test

Probabilistic Failure Propagation and Transformation Analysis	215
<i>Xiaocheng Ge, Richard F. Paige, and John A. McDermid</i>	
Towards Model-Based Automatic Testing of Attack Scenarios.....	229
<i>M. Zulkernine, M.F. Raihan, and M.G. Uddin</i>	

CRIOP: A Human Factors Verification and Validation Methodology That Works in an Industrial Setting	243
<i>Andreas Lumbe Aas, Stig Ole Johnsen, and Torbjørn Skramstad</i>	

Fault Tolerance

Reliability Analysis for the Advanced Electric Power Grid: From Cyber Control and Communication to Physical Manifestations of Failure	257
<i>Ayman Z. Faza, Sahra Sedigh, and Bruce M. McMillin</i>	
Increasing the Reliability of High Redundancy Actuators by Using Elements in Series and Parallel	270
<i>Thomas Steffen, Frank Schiller, Michael Blum, and Roger Dixon</i>	
AN-Encoding Compiler: Building Safety-Critical Systems with Commodity Hardware	283
<i>Christof Fetzer, Ute Schiffel, and Martin Süßkraut</i>	

Dependability

Component-Based Abstraction in Fault Tree Analysis	297
<i>Dominik Domis and Mario Trapp</i>	
A Foundation for Requirements Analysis of Dependable Software	311
<i>Denis Hatebur and Maritta Heisel</i>	
Establishing a Framework for Dynamic Risk Management in 'Intelligent' Aero-Engine Control	326
<i>Zeshan Kurd, Tim Kelly, John McDermid, Radu Calinescu, and Marta Kwiatkowska</i>	

Author Index	343
-------------------------------	-----