Lecture Notes in Computer Science 5775

Bettina Buth   Gerd Rabe   Till Seyfarth (Eds.)

Computer Safety, Reliability, and Security

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

Springer

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

springer.com

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

Safety Guidelines

Automotive

Aerospace

Verification, Validation, Test

Fault Tolerance

Dependability