Lecture Notes in Computer Science 3219

Maritta Heisel Peter Liggesmeyer
Stefan Wittmann (Eds.)

Computer Safety, Reliability, and Security

23rd International Conference, SAFECOMP 2004
Potsdam, Germany, September 21-24, 2004
Proceedings

Springer

Volume Editors

Maritta Heisel
Westfälische Wilhelms-Universität Münster
Institut für Informatik
Einsteinstr. 62, 48149 Münster, Germany
E-mail: heisel@uni-muenster.de

Peter Liggesmeyer
Fraunhofer Institut Experimentelles Software Engineering
Sauerwiesen 6, 67661 Kaiserslautern, Germany
E-mail: Peter.Liggesmeyer@t-online.de

Stefan Wittmann
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn, Germany
E-mail: stefan.wittmann@bsi.bund.de

Library of Congress Control Number: 2004112221

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

ISSN 0302-9743
ISBN 3-540-23176-5 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11317234 06/3142 5 4 3 2 1 0

Preface

The importance of safety and security is growing steadily. Safety is a quality characteristic that traditionally has been considered to be important in embedded systems, and security is usually an essential property in business applications. There is certainly a tendency to use software-based solutions in safety-critical applications domains, which increases the importance of safety engineering techniques. These include modelling and analysis techniques as well as appropriate processes and tools. And it is surely correct that the amount of confidential data that require protection from unauthorized access is growing. Therefore, security is very important. On the one hand, the traditional motivations for addressing safety and security still exist, and their relevance has improved. On the other hand, safety and security requirements occur increasingly in the same system. At present, many software-based systems interact with technical equipment and they communicate, e.g., with users and other systems. Future systems will more and more interact with many other entities (technical systems, people, the environment). In this situation, security problems may cause safety-related failures. It is thus necessary to address safety *and* security. It is furthermore required to take into account the interactions between these two properties.

Since their start in 1979 the SAFECOMP conferences have provided a platform for discussing topics related to dependable applications of computer systems. This requires us to deal with system aspects including hardware and software. Additionally, it is necessary to address a variety of properties, e.g., safety, security, reliability, and availability. The SAFECOMP conferences discuss research results, technical innovations, tools, processes, and organizational aspects. And they provide a forum for exchanging ideas between researchers and industry.

This year's program underlined system aspects. The majority of the contributions presented approaches that address complete systems including hardware, software, and the environment. The technical content covered a wide range from formal to informal methods. It seems that each approach is characterized by specific preconditions and has its own application domain.

We are convinced that the reader of this book will get valuable information on how to improve the safety and security of computer-based systems.

Authors from 17 countries all over the world responded to the call for papers. Out of 63 submitted papers, 24 were selected for the conference. We wish to thank the members of the International Programme Committee and the external reviewers for their excellent review work and fruitful discussions in setting up the programme of SAFECOMP 2004. They also helped a lot to disseminate all announcements.

We would like to express our special thanks to Massimo Felici. He maintained the tool CyberChair for us, and, being the organizer of the last two

SAFECOMPs, he was our oracle and early warning system of what could possibly go wrong.

Sincere thanks go to the invited speakers, Andreas Pfitzmann, Didier Essamé and Ralf G. Herrtwich, and the session chairpersons for their support.

Setting up the technical programme of the conference was one thing, to actually make SAFECOMP 2004 happen was another. Our organizing team Katrin Augustin, Hans-Peter Wagner, Carsten von Schwichow and Holger Schmidt did their best to make this event a success, and they did an outstanding job. Thank you.

Last but not least our special thanks go to the Hasso-Plattner-Institute in Potsdam for providing the premises, the conference infrastructure and the answers to all our questions.

Our best wishes go to the organizers of SAFECOMP 2005 in Norway, and we hope that SAFECOMP 2004 motivated many attendees to support next year's conference.

Potsdam, Germany
July 2004

Peter Liggesmeyer
Maritta Heisel
Stefan Wittmann

Organization

General Chair

Peter Liggesmeyer, Germany

Programme Co-chairs

Maritta Heisel, Germany
Stefan Wittmann, Germany

EWICS TC7 Chair

Udo Voges, Germany

Organizing Committee

Katrin Augustin, Germany
Hans-Peter Wagner, Germany

International Programme Committee

S. Anderson, UK
H. Bezecny, Germany
R. Bharadwaj, USA
R. Bloomfield, UK
S. Bologna, Italy
A. Bondavalli, Italy
B. Buth, Germany
P. Daniel, UK
M. Felici, UK
R. Genser, Austria
C. Goring, UK
J. Gorski, Poland
B.A. Gran, Norway
W. Grieskamp, Germany
E. Großpietsch, Germany
W. Halang, Germany
M. Heiner, Germany
M. Heisel, Germany
C. Heitmeyer, USA
C. Johnson, UK
M. Kaâniche, France
K. Kanoun, France
F. Koob, Germany
F. Koornneef, The Netherlands
B. Krämer, Germany
D. Kügler, Germany
P. Ladkin, Germany
P. Liggesmeyer, Germany
O. Mäckel, Germany
M. v.d. Meulen, UK
O. Nordland, Norway
A. Pasquini, Italy
G. Rabe, Germany
F. Redmill, UK
M. Rothfelder, Germany
J. Rushby, USA
F. Saglietti, Germany
T. Santen, Germany
E. Schoitsch, Austria
J. Souquières, France
W. Stephan, Germany
L. Strigini, UK
M. Sujan, UK
P. Traverso, Italy
J. Trienikens, The Netherlands
M. Ullmann, Germany
U. Voges, Germany
A. Weinert, Germany
M. Wilikens, Italy
R. Winther, Norway
S. Wittmann, Germany
E. Wong, USA
Z. Zurakowski, Poland

External Reviewers

C.P. van Beers
R. Carvajal-Schiaffino
I. Eusgeld
J. Jacky
H. Kelter
C. Kollmitzer
J. Krinke
J. Lei
R. Leszczyna
J. Li
P. Lollini
A. Nonnengart
S. Pozzi
G. Rock
M. Roveri
L. Save
H. Schwigon
D. Sona
N. Tillmann
A. Villafiorita

Table of Contents

Invited Talk

Safety Cases

Reliability

Human Factors

Invited Talk

Transportation

Software Development

Fault Tree Analysis

Invited Talk

Formal Methods and Systems

Security and Quality of Service

Hazard and Risk Analysis