Lecture Notes in Computer Science 1516
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Wolfgang Ehrenberger (Ed.)

Computer Safety, Reliability and Security

17th International Conference, SAFECOMP'98
Heidelberg, Germany, October 5-7, 1998
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Wolfgang Ehrenberger
Fachhochschule Fulda
Fachbereich Angewandte Informatik
Postfach 12 69, D-36012 Fulda, Germany
E-mail: ehrenberger@informatik.fh-fulda.de

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Computer safety, reliability and security : 17th international conference ; proceedings / SAFECOMP '98, Heidelberg, Germany, October 5 - 7, 1998. Wolfgang Ehrenberger (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1516)
ISBN 3-540-65110-1

CR Subject Classification (1991): D.1-4, E.4, C.3, F.3, K.6.5

ISSN 0302-9743
ISBN 3-540-65110-1 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN: 10692744 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

Computers and their interactions are becoming the characteristic features of our time: Many people believe that the industrial age is going over into the information age. In the same way as life of the beginning of this century was dominated by machines, factories, streets and railways, the starting century will be characterised by computers and their networks. This change naturally affects also the institutions and the installations our lives depend upon: power plants, including nuclear ones, chemical plants, mechanically working factories, cars, railways and medical equipment; they all depend on computers and their connections. In some cases it is not human life that may be endangered by computer failure, but large investments; e.g. if a whole plant interrupts its production for a long time. In addition to loss of life and property one must not neglect public opinion, which is very critical in many countries against major technical defects.

The related computer technology, its hardware, software and production process differ between standard applications and safety related ones: In the safety case it is normally not only the manufacturers and the customers that are involved, but a third party, usually an assessor, who is taking care of the public interest on behalf of a state authority. Usually safety engineers are in a better position than their colleagues from the conventional side, as they may spend more time and money on a particular task and use better equipment. On the other hand, in addition to the costumer's wishes, they have to take into account the demands of assessors and regulators, who may reject their final product.

It has been the purpose of the SAFECOMP conference series to review the state of science and technology of safety related computing and provide a constructive exchange of ideas, opinions and visions among experts.

Since the SAFECOMP conferences have been running over nearly 20 years now, one may make some comparisons: This year's contributions are characterised by a large share of formal approaches and formal methods; it seems that deterministic views are coming to dominate over probabilistic ones. Another characteristic is that the hardware problems as such seem to be more or less solved; the contributions submitted in 1998 are dealing mainly with system aspects and with software aspects.

I hope that the reader of this book gets important information on how to make computer controlled systems safer at lower cost.

Fulda, Germany
August 1998 Wolfgang Ehrenberger

International Programme Committee

S. Anderson – UK
R. Bloomfield (EWICS Chair) - UK
F. Dafelmair - D
W. Ehrenberger (IPC Chair) - D
J. Gorski - PL
P. Joannou - CDN
F. Koornneef - NL
Ch. Mazuet - F
G. Rabe - D
B. Runge - DK
I. Smith - UK
H. Bezecny - D
S. Bologna - I
G. Dahll - N
H. Frey - CH
G. Hockey - UK
J. Järvi - FIN
R. Lauber - D;
M. van der Meulen - NL
J. Rainer - A
F. Saglietti - D
J. Zalewski - USA
P. Bishop - UK
G. Cleland - UK
P. Daniel - UK
R. Genser - A
D. Inverso - USA
K. Kanoun - F
V. Maggioli - USA
A. Pasquini - I
F. Redmill - UK
E. Schoitsch - A

Local Organising Committee

C. Harms R. Lauber H. Rampacher W. Ehrenberger

List of Contributors

R. Belschner
Daimler Benz AG
FT2/EA, HPC T721
D - 70546 Stuttgart

Piergiorgio Bertoli
Istituto per la Ricerca Scientifica
e Tecnologica (IST)
I - 38050 Povo, Trento

Gino Biondi
Ansaldo Segnalamento Ferroviario
Via dei Pescatori 35
I -16129 Genova

Sandro Bologna
ENEA C.R. Casaccia
Via Anguillarese 301
I - 00060 Roma

Rocco Bove
ENEA C.R. Casaccia
Via Anguillarese 301
I - 00060 Roma

Aarnout Brombacher
University of Technology
P.O. Box 513
NL - 5600 MB Eindhoven

Alessandro Cimatti
Istituto per la Ricerca Scientifica
e Tecnologica (IST)
I - 38050 Povo, Trento

Ferdinand J. Dafelmair
TÜV Energie- und Systemtechnik
Westend Street 199
D - 80686 Munich

Vincent David
LETI (CEA - Advanced
Technologies)
DEIN - CEA/Saclay
F - 91191 Gif sur Yvette Cedex

Jean Delcoigne
LETI (CEA - Advanced
Technologies)
DEIN - CEA/Saclay
F - 91191 Gif sur Yvette Cedex

Fokko van Dijk
Holland Railconsult
P.O. Box 2855
NL - 3500 GW Utrecht

E. Dilger
Robert Bosch GmbH
Postfach 106050
D - 70049 Stuttgart

Giovanni Dioppa
ENEA C.R. Casaccia
Via Anguillarese 301
I - 00060 Roma

Rolf Drechsler
Albert-Ludwigs-University
Institute of Computer Science
Am Flughafen 17
D - 79110 Freiburg im Breisgau

Wan Fokkink
University of Wales Swansea
Singleton Park
Swansea SA2 8PP
United Kingdom

Alceu Heinke Frigeri
Fachbereich Elektrotechnik
Fernuniversität
Elberfelderstrasse
D - 58095 Hagen

T. Führer
Robert Bosch GmbH
Postfach 106050
D - 70049 Stuttgart

W. Geisselhardt
Gerhard-Mercator-University
Duisburg
Dept. of Dataprocessing
Faculty of Electrical Engineering
D - 47057 Duisburg

Fausto Giunchiglia
Istituto per la Ricerca Scientifica
e Tecnologica (IST)
I - 38050 Povo, Trento

Janusz Gorski
Department of Applied Informatics
Technical University of Gdansk
Narutowicza 11/2
PL - 80-952 Gdansk

Timm Grams
Fachhochschule Fulda
Fachbereich Elektrotechnik
Marquardstraße 35
D - 36039 Fulda

S. Gritzalis
Department of Information and
Communication Systems
University of the Aegean
30 Voulgaroktonou Street
GR - 11472 Athens

Wolfgang Halang
Fachbereich Elektrotechnik
Fernuniversität
Elberfelderstraße
D - 58084 Hagen

B. Hedenetz
Daimler Benz AG
FT2/EA, HPC T721
D - 70546 Stuttgart

Maritta Heisel
Institut für Verteilte Systeme
Fakultät für Informatik
Otto-von-Guerike-Universität
Magdeburg
D - 39016 Magdeburg

H. Hilmer
Gerhard-Mercator-University
Dept. of Information Processing
Faculty of Mechanical Engineering
D - 47057 Duisburg

Philippe Hilsenkopf
Framatome IT/LA
Tour Framatome
F - 92400 Courbevoie

Kevin Hollingworth
Centre for Software Reliability
Department of Computing Science
University of Newcastle upon Tyne
NE1 7RU
United Kingdom

Andrew Hutchison
Department of Computer Science
University of Cape Town
Private Bag
7700 Rondebosch
South Africa

J. Iliadis
Department of Information and Communication Systems
University of the Aegean
30 Voulgaroktonou Street
GR - 11472 Athens

Peter Isacsson
Q-Labs AB
Ideon Research Park
S - 22370 Lund

Silvije Jovalekic
University of Applied Science
Jakobstraße 6
D - 72458 Albstadt

Jeff Joyce
Raytheon Systems Canada, Ltd.
13951 Bridgeport Road
CAN-Richmond, BC V6V 1J6
Canada

P. Kan
Department of Computing
Imperial College
180 Queens Gate
London SW7 2BZ
United Kingdom

Niels Kirkegaard
IFAD
Forskerparken 10
DK - 5230 Odense

Bert Knegtering
Honeywell Safety Management Systems
P.O. Box 116
NL - 5223 AS ‘s-Hertogenbosch

H.-D. Kochs
Gerhard-Mercator-University
Duisburg
Deptartmt. of Information Processing
Faculty of Mechanical Engineering
D - 47057 Duisburg

Gea Kolk
Holland Railconsult
PO Box 2855
NL - 3500 GW Utrecht

Floor Koornneef
Delft University of Technology
Safety Science Group
Kanaalweg 2b
NL - 2628 EB Delft

K. Lano
Department of Computing
Imperial College
180 Queens Gate
London SW7 2BZ
United Kingdom

M. Lenord
Gerhard-Mercator-University
Deptartmt. of Information Processing
Faculty of Mechanical Engineering
D - 47057 Duisburg

Evelyne Leret
EDF/DER
6, quai Watier
BP 49
F - 78401 Chatou

Peter Liggesmeyer
Corporate Technology
Siemens AG
Otto Hahn Ring 6
D - 81730 München

Arndt Lindner
Institut für Sicherheitstechnologie
Forschungsgelände
D - 85748 Garching

Nicolas Martin-Vivaldi
Q-Labs AB
Ideon Research Park
S - 22370 Lund

Agathe Merceron
Basser of Computer Science
University of Sydney
Madsen Building F09
Sydeney NSW 2006
Australia

Bas A. de Mol
Academic Medical Center
Deptmt. Cardiopulmonary Surgery
Meibergdreef 9
NL-1105 AZ Amsterdam Zuidoost

Giorgio Mongardi
Ansaldo Segnalamento Ferroviario
(ASF)
Via dei Pescatori 35
I - 16129 Genova

Benny Graft Mortensen
IFAD
Forskerparken 10
DK - 5230 Odense

B. Müller
Robert Bosch GmbH
Postfach 106050
D - 70049 Stuttgart

Monika Müllerburg
GMD
Schloss Birlinghoven
D - 53754 Sankt Augustin

Bartosz Nowicki
Department of Applied Informatics
Technical University of Gdansk
Narutowicza 11/2
PL - 80-952 Gdansk

V. Oikonomou
Department of Informatics
T.E.I of Athens
Ag.Spiridonos St.
GR - 12243 Aegaleo

Alain Ourghanlian
EDF/DER
6, quai Watier
BP 49
F - 78401 Chatou

Philippe Paris
Framatome IT/LA
Tour Framatome
F - 92400 Courbevoie

G. Michele Pinna
Dipartimento di Matematica
Universita degli Studi di Siena
Via del Capitano 15
I - 53100 Siena

Carmen Porzia
Ansaldo Segnalamento Ferroviario
Via dei pescatori, 35
I - 16129 Genova

Thomas Ringler
University of Stuttgart
Institstute for Industrial Automation
and Software Engineering
Pfaffenwaldring 47
D - 70569 Stuttgart

Bernd Rist
Eff-Eff Company
Joh.-Mauthe-Str. 14
D - 72458 Albstadt

Dario Romano
Ansaldo Segnalamento Ferroviario
(ASF)
Via dei Pescatori 35
I - 16129 Genova

Martin Rothfelder
Corporate Technology
Siemens AG
Otto Hahn Ring 6
D - 81730 München

Heinrich Rust
Lehrstuhl für Software Systemtechnik
BTU
Postfach 101344
D - 03013 Cottbus

Krysztof Sacha
Warsaw University of Technology
Institute of Control and Computation
Engineering
ul. Nowowiejeska 15/19
Pl - 00-665 Warszawa

Amer Saeed
Centre for Software Reliability
Department of Computing Science
University of Newcastle upon Tyne
NE1 7RU
United Kingdom

Francesca Saglietti
Institut für Sicherheitstechnologie
Forschungsgelände
D - 85748 Garching

A.Sanchez
CINVESTAV-Guadalajara
Abdo Postal 31-438
Guadalajara 45550
Mexico

Thomas Santen
Institut für Verteilte Systeme
Fakultät für Informatik
Otto-von-Guerike-Universität
D - 39016 Magdeburg

Erwin Schoitsch
Österreichisches Forschungszentrum
Seibersdorf
A - 2444 Seibersdorf

Gerald Sonneck
Österreichisches Forschungszentrum
Seibersdorf
A - 2444 Seibersdorf

J. Steiner
University of Stuttgart
Institute for Industrial Automation
and Software Engineering
Pfaffenwaldring 47
D-70569 Stuttgart

Lorenzo Strigini
Centre for Software Reliability
City University
Northampton Square
London EC1V 0HB
United Kingdom

Fernando Torielli
Ansaldo Segnalamento Ferroviario
(ASF)
Via dei Pescatori 35
I - 16129 Genova

Paolo Traverso
Istituto per la Ricerca Scientifica
e Tecnologica (IST)
I - 38050 Povo, Trento

Paul van de Ven
Holland Railconsult
P.O. Box 2855
NL - 3500 GW Utrecht

Bas van Vlijmen
Utrecht University
Heidelberglaan 8
NL - 3584 CS Utrecht

Michael Wallbaum
Department of Computer Science 4
University of Technology
Ahornstrasse 55
D - 52056 Aachen

Kirsten Winter
GMD FIRST
Rudower Chaussee 5
D - 12489 Berlin

Ken Wong
University of British Columbia
Department of Computer Science
CAN-Vancover, BC V6T 1Z4
Canada

Contents

Medical Informatics

Formal Methods II - Languages and Verification

Applications

List of Contributors

R. Belschner
Daimler Benz AG
FT2/EA, HPC T721
D - 70546 Stuttgart

Piergiorgio Bertoli
Istituto per la Ricerca Scientifica
e Tecnologica (IST)
I - 38050 Povo, Trento

Gino Biondi
Ansaldo Segnalamento Ferroviario
Via dei Pescatori 35
I -16129 Genova

Sandro Bologna
ENEA C.R. Casaccia
Via Anguillarese 301
I - 00060 Roma

Rocco Bove
ENEA C.R. Casaccia
Via Anguillarese 301
I - 00060 Roma

Aarnout Brombacher
University of Technology
P.O. Box 513
NL - 5600 MB Eindhoven

Alessandro Cimatti
Istituto per la Ricerca Scientifica
e Tecnologica (IST)
I - 38050 Povo, Trento

Ferdinand J. Dafelmair
TÜV Energie- und Systemtechnik
Westend Street 199
D - 80686 Munich

Vincent David
LETI (CEA - Advanced
Technologies)
DEIN - CEA/Saclay
F - 91191 Gif sur Yvette Cedex

Jean Delcoigne
LETI (CEA - Advanced
Technologies)
DEIN - CEA/Saclay
F - 91191 Gif sur Yvette Cedex

Fokko van Dijk
Holland Railconsult
P.O. Box 2855
NL - 3500 GW Utrecht

E. Dilger
Robert Bosch GmbH
Postfach 106050
D - 70049 Stuttgart

Giovanni Dioppa
ENEA C.R. Casaccia
Via Anguillarese 301
I - 00060 Roma

Rolf Drechsler
Albert-Ludwigs-University
Institute of Computer Science
Am Flughafen 17
D - 79110 Freiburg im Breisgau

Wan Fokkink
University of Wales Swansea
Singleton Park
Swansea SA2 8PP
United Kingdom

Alceu Heinke Frigeri
Fachbereich Elektrotechnik
Fernuniversität
Elberfelderstrasse
D - 58095 Hagen

T. Führer
Robert Bosch GmbH
Postfach 106050
D - 70049 Stuttgart

W. Geisselhardt
Gerhard-Mercator-University
Duisburg
Dept. of Dataprocessing
Faculty of Electrical Engineering
D - 47057 Duisburg

Fausto Giunchiglia
Istituto per la Ricerca Scientifica
e Tecnologica (IST)
I - 38050 Povo, Trento

Janusz Gorski
Department of Applied Informatics
Technical University of Gdansk
Narutowicza 11/2
PL - 80-952 Gdansk

Timm Grams
Fachhochschule Fulda
Fachbereich Elektrotechnik
Marquardstraße 35
D - 36039 Fulda

S. Gritzalis
Department of Information and
Communication Systems
University of the Aegean
30 Voulgaroktonou Street
GR - 11472 Athens

Wolfgang Halang
Fachbereich Elektrotechnik
Fernuniversität
Elberfelderstraße
D - 58084 Hagen

B. Hedenetz
Daimler Benz AG
FT2/EA, HPC T721
D - 70546 Stuttgart

Maritta Heisel
Institut für Verteilte Systeme
Fakultät für Informatik
Otto-von-Guerike-Universität
Magdeburg
D - 39016 Magdeburg

H. Hilmer
Gerhard-Mercator-University
Dept. of Information Processing
Faculty of Mechanical Engineering
D - 47057 Duisburg

Philippe Hilsenkopf
Framatome IT/LA
Tour Framatome
F - 92400 Courbevoie

Kevin Hollingworth
Centre for Software Reliability
Department of Computing Science
University of Newcastle upon Tyne
NE1 7RU
United Kingdom

Andrew Hutchison
Department of Computer Science
University of Cape Town
Private Bag
7700 Rondebosch
South Africa

J. Iliadis
Department of Information and Communication Systems
University of the Aegean
30 Voulgaroktonou Street
GR - 11472 Athens

Peter Isacsson
Q-Labs AB
Ideon Research Park
S - 22370 Lund

Silvije Jovalekic
University of Applied Science
Jakobstraße 6
D - 72458 Albstadt

Jeff Joyce
Raytheon Systems Canada, Ltd.
13951 Bridgeport Road
CAN-Richmond, BC V6V 1J6
Canada

P. Kan
Department of Computing
Imperial College
180 Queens Gate
London SW7 2BZ
United Kingdom

Niels Kirkegaard
IFAD
Forskerparken 10
DK - 5230 Odense

Bert Knegtering
Honeywell Safety Management Systems
P.O. Box 116
NL - 5223 AS ‘s-Hertogenbosch

H.-D. Kochs
Gerhard-Mercator-University
Duisburg
Deptartmt. of Information Processing
Faculty of Mechanical Engineering
D - 47057 Duisburg

Gea Kolk
Holland Railconsult
PO Box 2855
NL - 3500 GW Utrecht

Floor Koornneef
Delft University of Technology
Safety Science Group
Kanaalweg 2b
NL - 2628 EB Delft

K. Lano
Department of Computing
Imperial College
180 Queens Gate
London SW7 2BZ
United Kingdom

M. Lenord
Gerhard-Mercator-University
Deptartmt. of Information Processing
Faculty of Mechanical Engineering
D - 47057 Duisburg

Evelyne Leret
EDF/DER
6, quai Watier
BP 49
F - 78401 Chatou

Peter Liggesmeyer
Corporate Technology
Siemens AG
Otto Hahn Ring 6
D - 81730 München

Arndt Lindner
Institut für Sicherheitstechnologie
Forschungsgelände
D - 85748 Garching

Nicolas Martin-Vivaldi
Q-Labs AB
Ideon Research Park
S - 22370 Lund

Agathe Merceron
Basser of Computer Science
University of Sydney
Madsen Building F09
Sydeney NSW 2006
Australia

Bas A. de Mol
Academic Medical Center
Deptmt. Cardiopulmonary Surgery
Meibergdreef 9
NL-1105 AZ Amsterdam Zuidoost

Giorgio Mongardi
Ansaldo Segnalamento Ferroviario
(ASF)
Via dei Pescatori 35
I - 16129 Genova

Benny Graft Mortensen
IFAD
Forskerparken 10
DK - 5230 Odense

B. Müller
Robert Bosch GmbH
Postfach 106050
D - 70049 Stuttgart

Monika Müllerburg
GMD
Schloss Birlinghoven
D - 53754 Sankt Augustin

Bartosz Nowicki
Department of Applied Informatics
Technical University of Gdansk
Narutowicza 11/2
PL - 80-952 Gdansk

V. Oikonomou
Department of Informatics
T.E.I of Athens
Ag.Spiridonos St.
GR - 12243 Aegaleo

Alain Ourghanlian
EDF/DER
6, quai Watier
BP 49
F - 78401 Chatou

Philippe Paris
Framatome IT/LA
Tour Framatome
F - 92400 Courbevoie

G. Michele Pinna
Dipartimento di Matematica
Universita degli Studi di Siena
Via del Capitano 15
I - 53100 Siena

Carmen Porzia
Ansaldo Segnalamento Ferroviario
Via dei pescatori, 35
I - 16129 Genova

Thomas Ringler
University of Stuttgart
Institstute for Industrial Automation
and Software Engineering
Pfaffenwaldring 47
D - 70569 Stuttgart

Bernd Rist
Eff-Eff Company
Joh.-Mauthe-Str. 14
D - 72458 Albstadt

Dario Romano
Ansaldo Segnalamento Ferroviario
(ASF)
Via dei Pescatori 35
I - 16129 Genova

Martin Rothfelder
Corporate Technology
Siemens AG
Otto Hahn Ring 6
D - 81730 München

Heinrich Rust
Lehrstuhl für Software Systemtechnik
BTU
Postfach 101344
D - 03013 Cottbus

Krysztof Sacha
Warsaw University of Technology
Institute of Control and Computation
Engineering
ul. Nowowiejeska 15/19
Pl - 00-665 Warszawa

Amer Saeed
Centre for Software Reliability
Department of Computing Science
University of Newcastle upon Tyne
NE1 7RU
United Kingdom

Francesca Saglietti
Institut für Sicherheitstechnologie
Forschungsgelände
D - 85748 Garching

A.Sanchez
CINVESTAV-Guadalajara
Abdo Postal 31-438
Guadalajara 45550
Mexico

Thomas Santen
Institut für Verteilte Systeme
Fakultät für Informatik
Otto-von-Guerike-Universität
D - 39016 Magdeburg

Erwin Schoitsch
Österreichisches Forschungszentrum
Seibersdorf
A - 2444 Seibersdorf

Gerald Sonneck
Österreichisches Forschungszentrum
Seibersdorf
A - 2444 Seibersdorf

J. Steiner
University of Stuttgart
Institute for Industrial Automation
and Software Engineering
Pfaffenwaldring 47
D-70569 Stuttgart

Lorenzo Strigini
Centre for Software Reliability
City University
Northampton Square
London EC1V 0HB
United Kingdom

Fernando Torielli
Ansaldo Segnalamento Ferroviario
(ASF)
Via dei Pescatori 35
I - 16129 Genova

Paolo Traverso
Istituto per la Ricerca Scientifica
e Tecnologica (IST)
I - 38050 Povo, Trento

Paul van de Ven
Holland Railconsult
P.O. Box 2855
NL - 3500 GW Utrecht

Bas van Vlijmen
Utrecht University
Heidelberglaan 8
NL - 3584 CS Utrecht

Michael Wallbaum
Department of Computer Science 4
University of Technology
Ahornstrasse 55
D - 52056 Aachen

Kirsten Winter
GMD FIRST
Rudower Chaussee 5
D - 12489 Berlin

Ken Wong
University of British Columbia
Department of Computer Science
CAN-Vancover, BC V6T 1Z4
Canada