Lecture Notes in Computer Science 1698

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Massimo Felici Karama Kanoun
Alberto Pasquini (Eds.)

Computer Safety, Reliability and Security

18th International Conference, SAFECOMP'99
Toulouse, France, September 27-29, 1999
Proceedings

Springer

Volume Editors

Massimo Felici
ENEA (sp 088)
Via Anguillarese, 301, I-00060 Roma, Italy
E-mail: felici@casaccia.enea.it

Karama Kanoun
LAAS-CNRS
7, Avenue du Colonel Roche, F-31077 Toulouse Cedex 4, France
E-mail: kanoun@laas.fr

Alberto Pasquini
ENEA (sp 088)
Via Anguillarese, 301, I-00060 Roma, Italy
E-mail: pasquini@casaccia.enea.it

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Computer safety, reliability and security : 18th international conference ; proceedings / SAFECOMP '99, Toulouse, France, September 27 - 29, 1999. Massimo Felici . . . (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1698)
ISBN 3-540-66488-2

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

ISSN 0302-9743
ISBN 3-540-66488-2 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10705000 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The European Commission emphasizes, in its Fifth Research Framework, the "...emerging generic dependability requirements in the information society, stemming both from the ubiquity and volume of embedded and networked systems and services as well as from the global and complex nature of large-scale information and communication infrastructures, from citizens, administrations and business in terms of technologies, tools, systems, applications and services". The series of Conference on Computer Safety, Reliability, and Security (Safecomp) contributes to satisfy these requirements by reviewing the state of the art, experiences, and new trends in the relevant scientific and industrial areas. Safecomp is intended to be a platform for technology transfer among academia, industry, and research institutions, providing the opportunity for exchange of ideas, opinions, and visions among experts.

This year Safecomp celebrates the 20th anniversary, its first Conference having been organized in Stuttgart by EWICS (European Workshop on Industrial Computer Systems) in 1979, and we hope these Proceedings will contribute to the celebration by supporting Safecomp aims. The Proceedings include the 25 papers that have been presented orally at the Conference and the full version of the 14 papers that have been presented as posters, all of which were selected from 76 submissions. Papers almost uniformly take up Safecomp topics, dealing with the issues of Safety Assessment and Human Factors, Verification and Validation, Design for Safety, Formal Methods, and Security.

As General and Program Chair of Safecomp '99, respectively, we would like to thank all authors who submitted their work, the presenters, the members of the international program committee and the local organising committee, the external reviewers, the session chairmen, the sponsors and co-sponsors, and all those who contributed to the Conference with their efforts and support.

We hope this book will prove to be useful reading, and help you in your research activity and in the design, assessment, and use of industrial computer systems.

Karama Kanoun
General Chair

Alberto Pasquini
IPC Chair

International Program Committee

S.	Anderson	UK	K.	Kanoun	F	(General Chair)
O.	Andersen	DK	F.	Koornneef	NL	
A.	Bertolino	I	V.	Maggioli	USA	
H.	Bezecny	D	C.	Mazet	F	
P.	Bishop	UK	C.	Mazuet	F	
R.	Bloomfield	UK	M.	Van der Meulen	NL	
S.	Bologna	I	A.	Pasquini	I	(IPC Chair)
F.	Cara	F	G.	Rabe	D	(EWICS Chair)
Y.	Crouzet	F	J.	Rainer	A	
F.	Dafelmair	D	F.	Redmill	UK	
W.	Ehrenberger	D	F.	Saglietti	D	
G.	Dahll	N	E.	Schoitsch	A	
P.	Daniel	UK	I.	Smith	UK	
R.	Genser	A	T.	Skramstad	NO	
J.	Gorski	PL	J.	Trienekens	NL	
D.	Inverso	USA	U.	Voges	D	
J.	Järvi	FIN	S.	Wittmann	D	
M.	Kaâniche	F	A. J.	Zalewski	USA	

Organizing Committee

Alain Costes, F
Yves Crouzet, F
Massimo Felici, I
Mohamed Kaâniche, F
Karama Kanoun, F
Marie-Thérèse Ippolito, F

External Reviewers

Gerard Duin, NL
Robert Garnier, F
Stefania Gnesi, I
Frank Koob, D
Raffaela Mirandola, I
Helmut Schwigon, D
Petra Scrivani, I
Peter van Sprundel, NL
Mark Sujan, D
Markus Ullmann, D
Jaap van Ekris, NL
Marja Visser, NL
Maria Wimmer, I

List of Contributors

Bernhard K. Aichernig
Technical University of Graz
Institute for Software Technology (IST)
Münzgrabenstr. 11/II
A-8010 Graz, Austria

Antonia Bertolino
Istituto di Elaborazione della Informazione, CNR
Via S. Maria, 46
56126 Pisa, Italy

Doo-Hwan Bae
Department of Computer Science, Korea Advanced Institute of Science and Technology, 373-1, Kusong-dong, Yusong-gu, Taejon 305-701, Korea

K. Bhattacharjiee
Reactor Control Division
Bhabha Atomic Research Centre
Mumbai 400 025, India

Yun Bai
School of Computing and Information Technology
University of Western Sydney Nepean
Australia

Jean-Paul Blanquart
LIS / LAAS-CNRS
7 avenue du Colonel Roche
31077 Toulouse Cedex 4, France

P. G. Beerthuizen
Fokker Space B. V.
Dept. ERA
Newtonweg 1, P.O.B. 32070
2303 DB Leiden, The Netherlands

Andrea Bobbio
Dipartimento di Scienze e Tecnologie Avanzate, Università del Piemonte Orientale "A. Avogadro" - C.so Borsalino 54 – 15100 Alessandria, Italy

Alfredo Benso
Politecnico di Torino
Dipartimento Automatica e Informatica
Corso Duca degli Abruzzi, 24
I-10129 Torino, Italy

José-Carlos Campelo
Department of Computer Engineering, Technical University of Valencia
Camino de Vera s/n, 46022 – Valencia
Spain

Cinzia Bernardeschi
Dipartimento di Ingegneria della Informazione, Università di Pisa
Via Diotisalvi, 2
56126 Pisa, Italy

Paul Caspi
VERIMAG
2 rue de Vignate
F-38610 Gières, France

Suong-Deok Cha
Department of Computer Science, Korea Advanced Institute of Science and Technology, 373-1, Kusong-dong, Yusong-gu, Taejon 305-701, Korea

Yves Crouzet
LIS / LAAS-CNRS
7 avenue du Colonel Roche
31077 Toulouse Cedex 4, France

A. Chiappini
Ansaldo Segnalamento Ferroviario
Via dei Pescatori
16100 Genova, Italy

Ireneusz Czarnowski
Gdynia Maritime Academy
ul. Morska 83
81-225 Gdynia, Poland

Ester Ciancamerla
ENEA – CRE Casaccia
Via Anguillarese, 301
00060 Roma, Italy

Gustav Dahll
Institute for Energy Technology
P.O. box 173
N-1751 Halden, Norway

A. Cimatti
IRST, Istituto per la Ricerca Scientifica e Tecnologica
Via Sommarive
Povo 38050 – Trento, Italy

Rogério de Lemos
Department of Computer Science
University of Newcastle upon Tyne
NE1 7RU, United Kingdom

Tim Clement
Adelard
Coborn House, 3 Coborn Road
London, E3 2DA, United Kingdom

Yves Deswarte
LAAS-CNRS
7 avenue du Colonel Roche
31077 Toulouse Cedex 4, France

Pierre Corneillie
CR2A-DI
25 quai Gallieni
92158 Suresnes cedex, France

S. D. Dhodapkar
Reactor Control Division
Bhabha Atomic Research Centre
Mumbai 400 025, India

Ian Cottam
Adelard
Coborn House, 3 Coborn Road
London, E3 2DA, United Kingdom

David Eames
ASACS Safety and Standards Unit
RAF
United Kingdom

Chin-Feng Fan
Department of Computer Engineering and Science, Yuan-Ze University
135 Far East Road
Chung-Li, Taiwan

Alessandro Fantechi
Dipartimento di Sistemi e Informatica
Università di Firenze
Via S. Marta, 3
50139 Firenze, Italy

Lucia Vilela Leite Filgueiras
Escola Politecnica da Universidade de Sao Paulo
C.P. 61548
05424-970, Sao Paulo, SP, Brazil

Peter Froome
Adelard
Coborn House, 3 Coborn Road
London, E3 2DA, United Kingdom

Pedro Gil
Department of Computer Engineering
Technical University of Valencia
Camino de Vera s/n 46022 – Valencia
Spain

Stefania Gnesi
Istituto di Elaborazione della Informazione, CNR
Via S. Maria, 46
56126 Pisa, Italy

John Goodson
Admiral Management Services Limited
Kings Court
91-93 High Strett Camberley
Surrey GU13 3RN, United Kingdom

Monika Heiner
Brandenburgische Technische Universität Cottbus
Institut für Informatik
D-03013 Cottbus, Germany

Maritta Heisel
Otto-von-Guericke-Universität Magdeburg, Fakultät für Informatik
Institut für Verteilte Systeme
D-39016 Magdeburg, Germany

Gordon Hughes
Department of Computer Science
University of Bristol
Woodland Road
Bristol BS8 1UB, United Kingdom

Andrew Hussey
Software Verification Research Centre
The University of Queensland
Brisbane, Qld, 4072, Australia

Yoon-Kyu Jang
Department of Computer Science
Korea Advanced Institute of Science and Technology 373-1, Kusong-dong
Yusong-gu, Taejon, 305-701, Korea

Piotr Jedrzejowicz
Gdynia Maritime Academy
ul. Morska 83
81-225 Gdynia, Poland

Chris Johnson
Department of Computer Science
University of Glasgow
Glasgow, G12 8QQ, United Kingdom

Claire Jones
Adelard
Coborn House, 3 Coborn Road
London, E3 2DA, United Kingdom

Mohamed Kaâniche
LAAS-CNRS
7 avenue du Colonel Roche
31077 Toulouse Cedex 4, France

Tim P. Kelly
Department of Computer Science
University of York
Heslington York, YO10 5DD
United Kingdom

Tai-Yun Kim
Department of Computer Science & Engineering, Korea University
1, 5-Ga Anam-Dong Seongbuk-Gu
Seoul 136-701, Korea

Heinrich Krebs
TÜV Rheinland
Am Grauen Stein
D-51105 Köln, Germany

W. Kruidhof
Fokker Space B. V.
Dept. ERA
Newtonweg 1, P.O.B. 32070
2303 DB Leiden, The Netherlands

Silke Kuball
Department of Computer Science
University of Bristol
Woodland Road
Bristol BS8 1UB, United Kingdom

Yong-Rae Kwon
Department of Computer Science
Korea Advanced Institute of Science and Technology 373-1, Kusong-dong
Yusong-gu, Taejon, 305-701, Korea

Sung-Min Lee
Department of Computer Science & Engineering, Korea University
1, 5-Ga Anam-Dong Seongbuk-Gu
Seoul 136-701, Korea

Gaetano Lombardi
Ericsson Telecomunicazioni SpA
Roma, Italy

Eda Marchetti
Istituto di Elaborazione della Informazione, CNR
Via S. Maria, 46
56126 Pisa, Italy

John May
Department of Computer Science
University of Bristol
Woodland Road
Bristol BS8 1UB, United Kingdom

Christine Mazuet
Schneider Electric
Usine M3
F-38050 Grenoble Cedex 9, France

John A. McDermid
Department of Computer Science
University of York
Heslington York, YO10 5DD
United Kingdom

Sang-Yoon Min
Department of Computer Science
Korea Advanced Institute of Science and Technology 373-1, Kusong-dong
Yusong-gu, Taejon, 305-701, Korea

Michele Minichino
ENEA – CRE Casaccia
Via Anguillarese, 301
00060 Roma, Italy

Raffaela Mirandola
Dipartimento di Informatica, Sistemi e Produzione
Università "Tor Vergata"
Roma, Italy

Swapan Mitra
Lloyds Register of Shipping
20 Wellesley Road
Croydon CR0 2AJ, United Kingdom

Jin Mo
LIS / LAAS-CNRS
7 avenue du Colonel Roche
31077 Toulouse Cedex 4, France

Jonathan Moffett
Department of Computer Science
University of York
Heslington York, YO10 5DD
United Kingdom

John D. Musa
Software Reliability Engineering and Testing Courses
39 Hamilton Road
Morristown, NJ 07960-5341, USA

Algirdas Pakstas
University of Sunderland
School of Computing Engineering and Technology, Chester Road
Sunderland SR1 3SD, United Kingdom

Yiannis Papadopoulos
Department of Computer Science
University of York
Heslington York, YO10 5DD
United Kingdom

Fabio Paternò
CNUCE – CNR
Via S. Maria, 36
56126 Pisa, Italy

Emilia Peciola
Ericsson Telecomunicazioni SpA
Roma, Italy

Peter Popov
Centre for Software Reliability
City University of London
Northampton Square
London EC1V OHB, United Kingdom

Luigi Portinale
Università del Piemonte Orientale "A. Avogadro"
C.so Borsalino, 54
15100 Alessandria, Italy

C. Porzia
Ansaldo Segnalamento Ferroviario
Via dei Pescatori
16100 Genova, Italy

Ewa Ratajczak
Gdynia Maritime Academy
ul. Morska 83
81-225 Gdynia, Poland

G. Rotondo
Ansaldo Segnalamento Ferroviario
Via dei Pescatori
16100 Genova, Italy

Maurizio Rebaudengo
Politecnico di Torino
Dip. di Automatica e Informatica
Corso Duca degli Abruzzi, 24
I-10129 Torino, Italy

Amer Saeed
Department of Computer Science
University of Newcastle upon Tyne
NE1 7RU, United Kingdom

Antonio Rizzo
Multimedia Communication Laboratory
University of Siena
Via dei Termini, 6
53100 Siena, Italy

Rym Salem
VERIMAG
2 rue de Vignate
F-38610 Gières, France

Philippe Robert
ISOscope
8, rue Maryse Hilsz
F-31500 Toulouse, France

Carmen Santoro
CNUCE – CNR
Via S. Maria, 36
56126 Pisa, Italy

Francisco Rodríguez
Department of Computer Engineering
Technical University of Valencia
Camino de Vera s/n 46022 – Valencia
Spain

Erwin Schoitsch
ARCS
A-2444 Seibersdorf, Austria

Laurence Rognin
Interaction Design Centre
Foundation Building
University of Limerick
Ireland

R. Sebastiani
IRST, Istituto per la Ricerca Scientifica e Tecnologica
Via Sommarive, Povo
38050 Trento, Italy

Alexander Romanovsky
Centre for Software Reliability
University of Newcastle-upon-Tyne
Newcastle upon Tyne NE1 7RU
United Kingdom

Kaisa Sere
Department of Computer Science
Turku Centre for Computer Science
Lemminkaisenkatu 14 A
FIN-20520 Turku, Finland

Juan-José Serrano
Department of Computer Engineering
Technical University of Valencia
Camino de Vera s/n 46022 – Valencia
Spain

Mark Sujan
Inst. f. Rechnerentwurf und Fehlertoleranz
University of Karlsruhe
Germany

Sanjit Seshia
School of Computer Science
Carnegie Mellon University
Pittsburgh PA 17217, USA

Sophie Tahmassebi
Centre d'Etudes de la Navigation Aérienne
Avenue Édouard Belin 7
31055 Toulouse Cedex, France

Igor Shagaev
Institute of Control Sciences
Profsoyuznaya St. 65
Moscow, Russia

P. Traverso
IRST, Istituto per la Ricerca Scientifica e Tecnologica
Via Sommarive, Povo
38050 Trento, Italy

R. K. Shyamasundar
School of Technology & Computer Science
Tata Institute of Fundamental Research
Mumbai 400 005, India

Elena Troubitsyna
Department of Computer Science
Turku Centre for Computer Science
Lemminkaisenkatu 14 A
FIN-20520 Turku, Finland

Gerald Sonneck
ARCS
A-2444 Seibersdorf, Austria

Gilles Trouessin
CNAMTS / CESSI
14 place St-Etienne
31000 Toulouse, France

Matteo Sonza Reorda
Politecnico di Torino
Dip. di Automatica e Informatica
Corso Duca degli Abruzzi, 24
I-10129 Torino, Italy

Vijay Varadharajan
School of Computing and Information Technology
University of Western Sydney Nepean
Australia

Lorenzo Strigini
Centre for Software Reliability
City University of London
Northampton Square
London EC1V OHB, United Kingdom

A. Villafiorita
IRST, Istituto per la Ricerca Scientifica e Tecnologica
Via Sommarive, Povo
38050 Trento, Italy

Daniel Weber
Schneider Electric
Usine M3
F-38050 Grenoble Cedex 9, France

Swu Yih
I&C Department
Institute of Nuclear Energy Research
P.O.Box 3-11
Lung-Yang, Taiwan

Maria Wimmer
Multimedia Communication Laboratory
University of Siena
Via dei Termini, 6
53100 Siena, Italy

Pedro Yuste
Department of Computer Engineering
Technical University of Valencia
Camino de Vera s/n 46022 – Valencia
Spain

Table of Contents

Invited Talk

Software Reliability Engineering in Industry 1
J. D. Musa

Assessment and Certification

A Systematic Approach to Safety Case Maintenance 13
T. P. Kelly, J. A. McDermid

SQUALE Dependability Assessment Criteria 27
Y. Deswarte, M. Kaâniche, P. Corneillie, and J. Goodson

Assessment and Certification of Safety-Critical Digital Architectures – the ACRuDA Project 39
G. Sonneck, E. Schoitsch

Safety Assessment and Human Factors (Poster Session)

Safety Evaluation of a Train Leader Telephone System 46
G. Dahll

Safety Analysis Techniques for Validating Formal Models during Verification 58
R. de Lemos, A. Saeed

Evaluating the Contribution of DesktopVR for Safety-Critical Applications 67
C. Johnson

Human Performance Reliability in the Design-for-Usability Life Cycle for Safety Human-Computer Interfaces 79
L. V. L. Filgueiras

The Impact of Different Media on Safety and Usability of Interactive ATC Applications 89
F. Paternò, C. Santoro, and S. Tahmassebi

Human Factors

Patterns for Safer Human-Computer Interfaces 103
A. Hussey

Impact of Communication on Systems Dependability:
Human Factors Perspectives 113
L. Rognin, J. P. Blanquart

A Method for Operator Error Detection Based on Plan Recognition.....125
J. Mo, Y. Crouzet

Safety Assessment

Hierarchically Performed Hazard Origin and Propagation Studies.....139
Y. Papadopoulos, J. A. McDermid

Hardware Redundant Vital Computers – Demonstration of Safety
on the Basis of Current Standards.....153
H. Krebs, S. Mitra

Design for Safety (Poster Session)

System and Software Safety Analysis for the ERA Control Computer 163
P.G. Beerthuizen, W. Kruidhof

Safety Markup Language: Concept and Application 177
C. F. Fan, S. Yih

Extendable Ground-to-Air Communication Architecture for CoDySa 187
A. Pakstas, I. Shagaev

Hierarchical Reliability and Safety Models of Fault Tolerant
Distributed Industrial Control Systems 202
J. C. Campelo, P. Yuste, F. Rodríguez, P. J. Gil, and J. J. Serrano

The Development of a Commercial “Shrink-Wrapped Application”
to Safety Integrity Level 2: the DUST-EXPERT™ Story 216
T. Clement, I. Cottam, P. Froome, and C. Jones

Verification and Testing

Safety Verification of ADA95 Programs Using Software Fault Trees 226
S. Y. Min, Y. K. Jang, S. D. Cha, Y. R. Kwon, and D. H. Bae

Programming Rule Static Verification for Reliable Software.....239
P. Robert

Automated Black-Box Testing with Abstract VDM Oracle 250
B. K. Aichernig

Towards Statistical Control of an Industrial Test Process.....260
G. Lombardi, E. Peciola, R. Mirandola, A. Bertolino, and E. Marchetti

Design for Safety

Choosing Effective Methods for Diversity – How to Progress from Intuition to Science 272
P. Popov, L. Strigini, and A. Romanovsky

A First Step Towards the Integration of Accident Reports and Constructive Design Documents 286
C. Johnson

A Holistic Design Concept to Improve Safety Related Control Systems 397
M. Wimmer, A. Rizzo, and M. Sujan

Dependability Analysis and Evaluation

Comparing Fault Trees and Bayesian Networks for Dependability Analysis 310
A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla

FlexFi: A Flexible Fault Injection Environment for Microprocessor-Based Systems 323
A. Benso, M. Rebaudengo, and M. S. Reorda

Structural Software Reliability Estimation.....336
S. Kuball, J. May, and G. Hughes

Formal Methods and Security (Poster Session)

Hazard Analysis in Formal Specification.....350
K. Sere, E. Troubitsyna

Modeling Safety-Critical Systems with Z and Petri Nets 361
M. Heiner, M. Heisel

On Formal Languages for Sequences of Authorization Transformations 375
Y. Bai, V. Varadharajan

Scheduling Fault-Tolerant Programs on Multiple Processors to Maximize Schedule Reliability 385
I. Czarnowski, P. Jedrzejowicz, and E. Ratajczak

Formal Methods

Forma Design of Distributed Control Systems with Lustre 396
P. Caspi, C. Mazuet, R. Salem, D. Weber

Formal Specification and Development of a
Safety-Critical Train Management System 410
A. Chiappini, A. Cimatti, C. Porzia, G. Rotondo, R. Sebastaini, P. Traverso, and A. Villafiorita

Formal Validation of the GUARDS Inter-consistency Mechanism 420
C. Bernardeschi, A. Fantechi, S. Gnesi

A Graphical Environment for the Specification and

Verification of Reactive Systems 431
A. K. Bhattacharjee, S. D. Dhodapkar, S. Seshia, and R. K. Shyamasundar

Security

Dependability Requirements and Security Architectures
for the Healthcare/Medical Sector 445
G. Trouessin

Three-Pass Hybrid Key Establishment Protocol Based on ESIGN Signature 459
S. M. Lee, T. Y. Kim

The Integration of Safety and Security Requirements 468
D. P. Eames, J. Moffett

Author Index 481