Computer Safety, Reliability and Security

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

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

## 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bernhard K. Aichernig</td>
<td>Technical University of Graz, Institute for Software Technology (IST)</td>
</tr>
<tr>
<td>Doo-Hwan Bae</td>
<td>Department of Computer Science, Korea Advanced Institute of Science and Technology</td>
</tr>
<tr>
<td>Yun Bai</td>
<td>School of Computing and Information Technology, University of Western Sydney Nepean Australia</td>
</tr>
<tr>
<td>P. G. Beerthuizen</td>
<td>Fokker Space B. V., Dept. ERA, Newtonweg 1, P.O.B. 32070, 2303 DB Leiden, The Netherlands</td>
</tr>
<tr>
<td>Alfredo Benso</td>
<td>Politecnico di Torino, Dipartimento Automatica e Informatica, Corso Duca degli Abruzzi, 24, I-10129 Torino, Italy</td>
</tr>
<tr>
<td>Cinzia Bernardeschi</td>
<td>Dipartimento di Ingegneria della Informazione, Università di Pisa, Via Diotisalvi, 2, 56126 Pisa, Italy</td>
</tr>
<tr>
<td>Antonia Bertolino</td>
<td>Istituto di Elaborazione della Informazione, CNR, Via S. Maria, 46, 56126 Pisa, Italy</td>
</tr>
<tr>
<td>K. Bhattacharjee</td>
<td>Reactor Control Division, Bhabha Atomic Research Centre, Mumbai 400 025, India</td>
</tr>
<tr>
<td>Jean-Paul Blanquart</td>
<td>LIS / LAAS-CNRS, 7 avenue du Colonel Roche, 31077 Toulouse Cedex 4, France</td>
</tr>
<tr>
<td>Andrea Bobbio</td>
<td>Dipartimento di Scienze e Tecnologie, Università del Piemonte Orientale “A. Avogadro” - C.so Borsalino 54 – 15100 Alessandria, Italy</td>
</tr>
<tr>
<td>José-Carlos Campelo</td>
<td>Department of Computer Engineering, Technical University of Valencia, Camino de Vera s/n, 46022 – Valencia, Spain</td>
</tr>
<tr>
<td>Paul Caspi</td>
<td>VERIMAG, 2 rue de Vignate, F-38610 Gières, France</td>
</tr>
</tbody>
</table>
Suong-Deok Cha  
Department of Computer Science, Korea Advanced Institute of Science and Technology, 373-1, Kusong-dong, Yusong-gu, Taejon 305-701, Korea

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

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

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

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

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

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

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

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

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

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

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

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

David Eames  
ASACS Safety and Standards Unit RAF United Kingdom
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
L. Rognin, J. P. Blanquart

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

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

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

Design for Safety (Poster Session)
System and Software Safety Analysis for the ERA Control Computer
P. G. Beerthuizen, W. Kruidhof

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

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

Hierarchical Reliability and Safety Models of Fault Tolerant Distributed Industrial Control Systems
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
T. Clement, I. Cottam, P. Froome, and C. Jones

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

Programming Rule Static Verification for Reliable Software
P. Robert

Automated Black-Box Testing with Abstract VDM Oracle
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
## Table of Contents

### Formal Methods

Formal 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