Lecture Notes in Computer Science 1943
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Floor Koornneef   Meine van der Meulen   (Eds.)

# Computer Safety, Reliability and Security

19th International Conference, SAFECOMP 2000
Rotterdam, The Netherlands, October 24-27, 2000
Proceedings

Springer

Series Editors

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

Volume Editors

Floor Koornneef
TU Delft, Safety Science Group
Jaffalaan 5, 2628 BX Delft, The Netherlands
E-mail: f.koornneef@tbm.tudelft.nl

Meine van der Meulen
SIMTECH
Max Euwelaan 60, 3062 MA Rotterdam, The Netherlands
E-mail: m.van.der.meulen@simtech.nl

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Computer safety, reliability and security : 19th international
conference ; proceedings / SAFECOMP 2000, Rotterdam, The Netherlands,
October 24 - 27, 2000. Floor Koornneef ; Meine van der Meulen (ed.). -
Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1943)
ISBN 3-540-41186-0

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

ISSN 0302-9743
ISBN 3-540-41186-0 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN: 10780880 06/3142 5 4 3 2 1 0

# Preface

Welcome to Rotterdam and to the International Conference Safecomp 2000, on the reliability, safety and security of critical computer applications. This already marks the 19th year of the conference, showing the undiminished interest the topic elicits from both academia and industry. Safecomp has proven to be an excellent place to meet and have discussions, and we hope this trend continues this year.

People and organisations depend more and more on the functioning of computers. Whether in household equipment, telecommunication systems, office applications, banking, people movers, process control or medical systems, the often-embedded computer subsystems are meant to let the hosting system realise its intended functions. The assurance of proper functioning of computers in dependable applications is far from obvious. The millennium started with the bug and the full endorsement of the framework standard IEC 61508. The variety of dependable computer applications increases daily, and so does the variety of risks related to these applications. The assessment of these risks therefore needs reflection and possibly new approaches. This year's Safecomp provides a broad mix of papers on these issues, on progress made in different application domains and on emerging challenges.

One of the special topics this year is *transport and infrastructure*. One would be hard pressed to find a better place to discuss this than in Rotterdam. The reliability, safety and security of computers is of prominent importance to Rotterdam, as a few examples illustrate. Its harbour depends on the reliable functioning of container handling systems, on the safe functioning of its radar systems, and, as of recently, on the safe and reliable functioning of the enormous storm surge barrier at Hoek van Holland.

A new topic for Safecomp is *medical systems*. These progressively depend on – embedded – programmable electronic systems. Experience shows that the medical world lacks the methods for applying these systems safely and reliably. We welcome a group of people ready to discuss this topic, and hope, by doing so, to contribute to this field of applications of safe, reliable and secure systems.

*Software process improvement* also represents a special topic of Safecomp 2000. It proved to be the most fruitful of the three in terms of submitted papers. There were many contributions from a host of countries, which had to be spread amongst different session topics.

We wish to thank the International Program Committee's members, 41 in total, for their efforts in reviewing the papers and for their valuable advice in organising this conference. We are also grateful for their contribution to distributing calls for papers and announcements. Without their help the burden of organising this conference would have been much greater.

Finally, let us once again welcome you to Rotterdam, a truly international city and home to people of many nationalities. We hope you take the time not only to enjoy this conference, but also to find your way around the city, since it surely has much to offer.

Floor Koornneef
Meine van der Meulen

# Table of Contents

**Invited Paper**

The Ten Most Powerful Principles for Quality in (Software and) Software Organizations for Dependable Systems .......... 1
*Tom Gilb*

**Verification and Validation**

Empirical Assessment of Software On-Line Diagnostics Using Fault Injection .......... 14
*John Napier, John May and Gordon Hughes*

Speeding-Up Fault Injection Campaigns in VHDL Models .......... 27
*B. Parrotta, M. Rebaudengo, M. Sonza Reorda and M. Violante*

Specification and Verification of a Safety Shell with Statecharts and Extended Timed Graphs .......... 37
*Jan van Katwijk, Hans Toetenel, Abd-El-Kader Sahraoui, Eric Anderson and Janusz Zalewski*

Validation of Control System Specifications with Abstract Plant Models .......... 53
*Wenhui Zhang*

A Constant Perturbation Method for Evaluation of Structural Diversity in Multiversion Software .......... 63
*Luping Chen, John May and Gordon Hughes*

Expert Error: The Case of Trouble-Shooting in Electronics .......... 74
*Denis Besnard*

The Safety Management of Data-Driven Safety-Related Systems .......... 86
*A. G. Faulkner, P. A. Bennett, R. H. Pierce, I. H. A. Johnston and N. Storey*

Software Support for Incident Reporting Systems in Safety-Critical Applications .......... 96
*Chris Johnson*

**Software Process Improvement**

A Dependability-Explicit Model for the Development of Computing Systems .......... 107
*Mohamed Kaâniche, Jean-Claude Laprie and Jean-Paul Blanquart*

Deriving Quantified Safety Requirements in Complex Systems ............ 117
*Peter A. Lindsay, John A. McDermid and David J. Tombs*

Improving Software Development by Using Safe Object Oriented Development: OTCD ............................... 131
*Xavier Méhaut and Pierre Morère*

A Safety Licensable PES for SIL 4 Applications ........................... 141
*Wolfgang A. Halang, Peter Vogrin and Matjaž Colnarič*

Safety and Security Issues in Electric Power Industry ..................... 151
*Zdzisław Żurakowski*

Dependability of Computer Control Systems in Power Plants ............. 165
*Cláudia Almeida, Alberto Arazo, Yves Crouzet and Karama Kanoun*

A Method of Analysis of Fault Trees with Time Dependencies ............ 176
*Jan Magott and Paweł Skrobanek*

**Formal Methods**

A Formal Methods Case Study: Using Light-Weight VDM for the Development of a Security System Module ........................ 187
*Georg Droschl, Walter Kuhn, Gerald Sonneck and Michael Thuswald*

Formal Methods: The Problem Is Education .............................. 198
*Thierry Scheurer*

Formal Methods Diffusion: Past Lessons and Future Prospects ............ 211
*R. Bloomfield, D. Craigen, F. Koob, M. Ullmann and S.Wittmann*

**Invited Paper**

Safe Tech: A Control Oriented Viewpoint ................................. 227
*Maarten Steinbuch*

**Safety Guidelines, Standards and Certification**

Derivation of Safety Targets for the Random Failure of Programmable Vehicle Based Systems .................................. 240
*Richard Evans and Jonathan Moffett*

IEC 61508 – A Suitable Basis for the Certification of Safety-Critical Transport-Infrastructure Systems?? ..................... 250
*Derek Fowler and Phil Bennett*

**Hardware Aspects**

An Approach to Software Assisted Recovery from Hardware Transient Faults for Real Time Systems ... 264
*D. Basu and R. Paramasivam*

Programmable Electronic System Design & Verification Utilizing DFM ... 275
*Michel Houtermans, George Apostolakis, Aarnout Brombacher and Dimitrios Karydas*

SIMATIC S7-400F/FH: Safety-Related Programmable Logic Controller ... 286
*Andreas Schenk*

**Safety Assessment I**

Assessment of the Reliability of Fault-Tolerant Software: A Bayesian Approach ... 294
*Bev Littlewood, Peter Popov and Lorenzo Strigini*

Estimating Dependability of Programmable Systems Using BBNs ... 309
*Bjørn Axel Gran, Gustav Dahll, Siegfried Eisinger, Eivind J. Lund, Jan Gerhard Norstrøm, Peter Strocka and Britt J. Ystanes*

**Design for Safety**

Improvements in Process Control Dependability through Internet Security Technology ... 321
*Ferdinand J. Dafelmair*

A Survey on Safety-Critical Multicast Networking ... 333
*James S. Pascoe and R. J. Loader*

**Invited Paper**

Causal Reasoning about Aircraft Accidents ... 344
*Peter B. Ladkin*

**Transport & Infrastructure**

Controlling Requirements Evolution: An Avionics Case Study ... 361
*Stuart Anderson and Massimo Felici*

HAZOP Analysis of Formal Models of Safety-Critical Interactive Systems ... 371
*Andrew Hussey*

Failure Mode and Effect Analysis for Safety-Critical Systems with Software Components ........ 382
*Tadeusz Cichocki and Janusz Górski*

**Safety Assessment II**

Risk Ordering of States in Safecharts ........ 395
*Nimal Nissanke and Hamdan Dammag*

Dependability Evaluation: Model and Method Based on Activity Theory .. 406
*Mark-Alexander Sujan, Antonio Rizzo and Alberto Pasquini*

Forensic Software Engineering and the Need for New Approaches to Accident Investigation ........ 420
*Chris Johnson*

**Author Index** ........ 431